Zigbee®数据包分析

AN4815

产品页链接

简介

本应用笔记详细介绍了如何配置和使用支持的嗅探工具以及基于 Microchip MCU 的嗅探器硬件平台。在 Zigbee®网络中，嗅探工具（如 Wireshark Network Protocol Analyzer（简称 Wireshark））用于捕捉和分析网络中交换的帧，在开发和测试阶段至关重要。在包含不同厂商 Zigbee 产品的网络中，由于产品间需实现互操作性，因此使用 Wireshark 进行测试和验证尤为重要。本应用笔记主要重点介绍使用 Wireshark 进行数据包捕捉的方法。

Wireshark 是一款免费开源的数据包分析器。通过在 PC 上运行 Wireshark，即可搭建无线网络嗅探环境。Wireshark 的用途如下：

- 网络故障排查
- 分析
- 软件和通信协议开发
- 教学培训

Wireshark Sniffer Interface Tool（Wireshark 嗅探器接口工具）负责连接 Wireshark 图形用户界面（Graphical User Interface，GUI）与运行在 ZigBit USB 设备上的嗅探器固件。这样，运行在 PC 上的 Wireshark Sniffer Interface Tool 应用程序便可与嗅探器硬件进行通信。Wireshark Sniffer Interface Tool 能够实时捕捉 Zigbee 协议和 IEEE® 802.15.4 标准支持的帧格式，并解析帧内各字段与子字段信息，帮助用户快速完成分析。

特性

- 网络拓扑
- 添加时间戳
- 多信道捕捉

目录

1. 快速参考

1.1. 参考文档

有关详细信息，请参见以下文档：

- *AT08550：ZigBee Attribute Reporting Application Note*（42334）
- *Atmel AT02597：ZigBee PRO Packet Analysis with Sniffer Application Note*（32210）
- *Atmel-ICE Programmers and Debuggers User Guide*（42330）
- *PRO Base Device Behavior Specification*（3.0.1）
- *ZigBee Alliance Cluster Library Specification Revision 8*（075123）
- *Matter Device Library Specification*（1.0）
- *Zigbee PRO Green Power feature specification Basic functionality set*（Version 1.1.1）
- *Zigbee Specification Revision 22 1.0*（05-3474-22）
- *ZigBit USB Stick User Guide*（42194）

1.2. 硬件要求

- 50-mil 10 引脚 IDC 扁平线缆
- ATMEL-ICE（ATATMEL-ICE）
- ATXMEGA256A3U 和 AT86RF212B ZIGBIT USB 设备（ATZB-X-212B-USB）
- ATXMEGA256A3 和 AT86RF233 ZIGBIT USB 设备（ATZB-X-233-USB）
- Micro-AB USB 线缆

1.3. 软件要求

- Microchip Studio（7.0.2594）
- Windows® 10
- Wireshark（3.6.8）
- Wireshark Sniffer Interface Tool（v3.0.0.10）

1.4. 缩略语与缩写

表 1-1. 缩略语与缩写

缩略语与缩写	说明
API	应用程序编程接口（Application Programming Interface）
APL	应用层（Application Layer）
APS	应用支持子层（Application Support Sub-Layer）
BDB	基础设备行为（Base Device Behavior）
GP	绿色能量（Green Power）
GPC	绿色能量组合（Green Power Combo）
GPD	绿色能量设备（Green Power Device）
GPP	绿色能量代理（Green Power Proxy）
GPS	绿色能量接收端（Green Power Sink）
GUI	图形用户界面（Graphical User Interface）
NWK	网络（Network）
PAN	个人局域网（Personal Area Network）

表 1-1. 缩略语与缩写 （续）

缩略语与缩写	说明
USB	通用串行总线（Universal Serial Bus）
ZCL	Zigbee®簇库（Zigbee Cluster Library）
ZDO	Zigbee 设备对象（Zigbee Device Object）
ZDP	Zigbee 设备配置文件（Zigbee Device Profile）

2. Wireshark Network Protocol Analyzer 和 Wireshark Sniffer Interface Tool 概述

本章概述了 Wireshark Network Protocol Analyzer（Wireshark）和 Wireshark Sniffer Interface Tool 的设置及其各自的组件。默认情况下，Wireshark 和 Wireshark Sniffer Interface Tool 分别将软件包安装在 *C:\Program Files*\和 *C:\Program Files (x86)*\路径下。

表 2-1. Wireshark 软件包文件

文件名	说明
`Wireshark-winXX-3.X.X.exe` 文件	Wireshark 可执行文件

表 2-2. Wireshark Sniffer Interface Tool 软件包文件

文件名/文件夹名称		说明
`Wireshark Sniffer Interface Tool v3.0.0.10.exe`		Wireshark Sniffer Interface Tool 可执行文件
C:\Program Files (x86)\Atmel\Atmel Wireshark Sniffer Interface Tool Folder	Atmel Wireshark 嗅探器固件	—
	`Atmel_Wireshark_Sniffer_Interface.exe`	Wireshark Sniffer Interface Tool 可执行文件
	`Atmel_Wireshark_Sniffer_Interface.exe.config`	Atmel Wireshark Sniffer Interface 框架配置文件
	`Release Notes.txt`	• 包含 Wireshark Sniffer Interface Tool 的发布和版本信息 • 用于捕捉/嗅探 IEEE® 802.15.4 帧（2.4 GHz 和 Sub-GHz）
	`System.Xaml.dll`	—
C:\Program Files (x86)\Atmel\Atmel Wireshark Sniffer Interface Tool\Atmel Wireshark Sniffer Firmware Folder	`AWSI_at32uc3a3256s_rz600_at86rf212.hex`	用于 RZ600 USB 设备的嗅探器固件。有关详细信息，请参见 ATAVRRZ600。
	`AWSI_at32uc3a3256s_rz600_at86rf231.hex`	
	`AWSI_atxmega256a3u_rf212b_zigbit_usb.hex`	用于 Sub-GHz 的 ZigBit USB 设备固件
	`AWSI_atxmega256a3u_rf233_zigbit_usb.hex`	用于 2.4 GHz 嗅探器的 ZigBit USB 设备固件

2.1. 支持的嗅探器硬件平台

若要开始在 IEEE 802.15.4 信道上捕捉帧，用户必须将运行嗅探器固件的嗅探器硬件工具插入 PC。以下是支持的嗅探器硬件平台：

- RF212B ZigBit USB 设备——用于嗅探 IEEE 802.15.4 Sub-GHz 信道
- RF233 ZigBit USB 设备——用于嗅探 IEEE 802.15.4 2.4 GHz 信道

图 2-1. 支持的嗅探器硬件平台——ZigBit USB 设备（RF212B/RF233——Sub-GHz/2.4 GHz）

使用 Wireshark Sniffer Interface Tool 为 2.4 GHz 和 Sub-GHz 范围内的 IEEE 802.15.4 信道创建捕捉会话。Wireshark Sniffer Interface Tool 支持 ATXMEGA256A3U_RF212B 和 ATXMEGA256A3U_RF233。

2.2. Wireshark 工具和 Wireshark Sniffer Interface Tool 入门

2.2.1. Wireshark 安装步骤

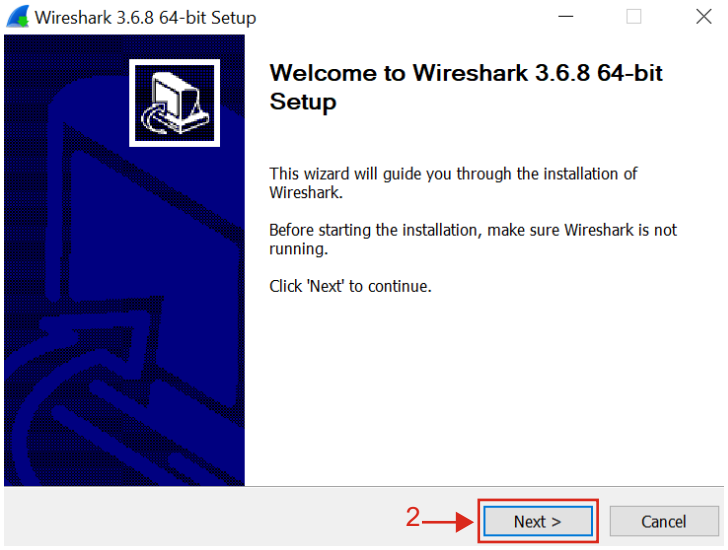
若要下载 Wireshark，请访问 Wireshark。有关 Wireshark 的详细信息，请访问 Wireshark。

注：Wireshark 的稳定发布版本为 3.6.6，用户也可以从 Wireshark 官方网站获取最新开发版本并在 PC 上进行安装。

以下是安装 Wireshark 的步骤：

1. 双击 `Wireshark-winXX-3.X.X.exe` 以启动安装过程。
2. 单击 **Next**（下一步）继续。

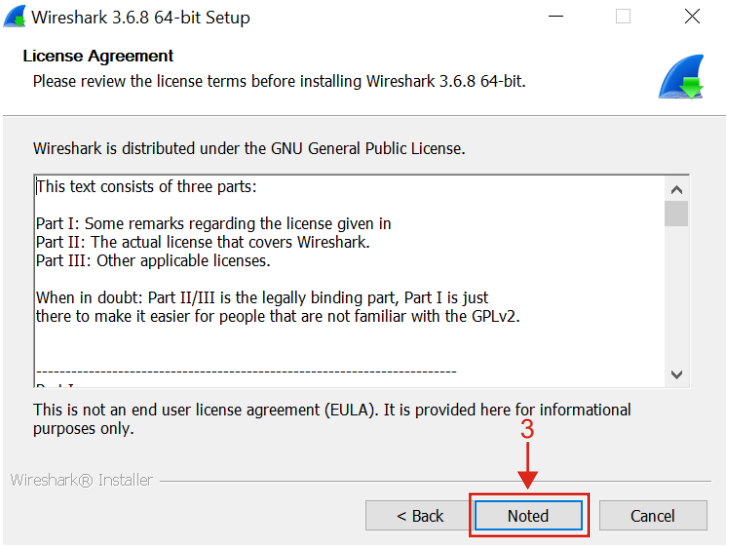
图 2-2. Wireshark 安装窗口



注：用户可使用最新版 Wireshark。

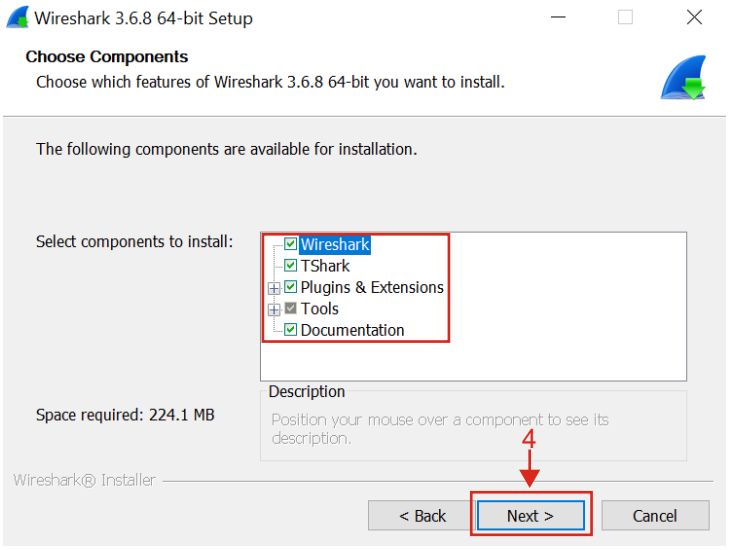
3. 单击 **Noted**（确认）继续。

图 2-3. Wireshark——许可协议



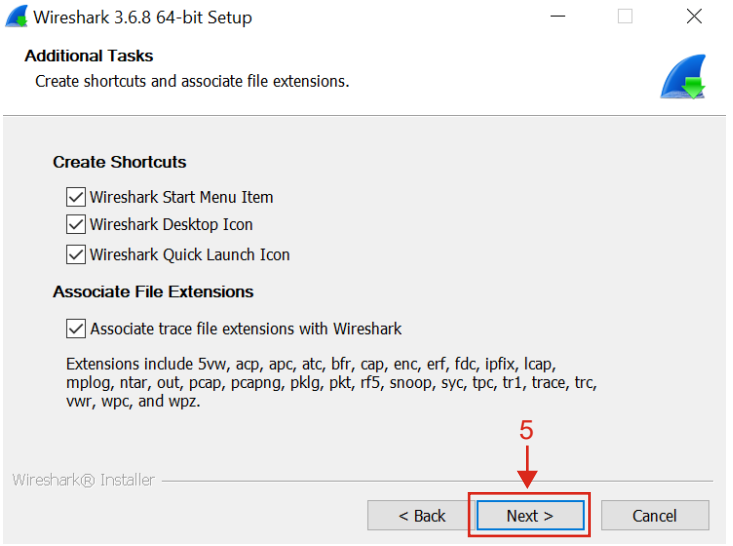
4. 在“Select components to install：”（选择要安装的组件：）字段下，选中要随该工具一起安装的组件。单击 **Next** 继续。

图 2-4. Wireshark——选择组件



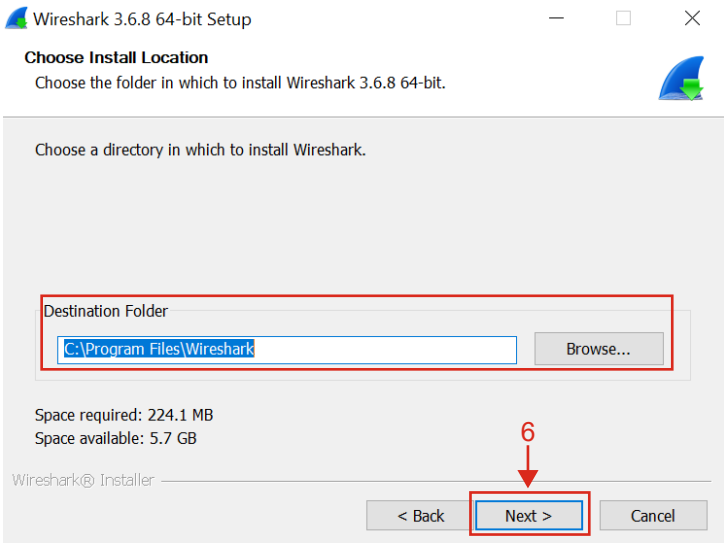
5. 在 **Create Shortcuts**（创建快捷方式）字段下选中所需的快捷方式，然后在 **Associate File Extensions**（关联文件扩展名）字段下选中 *Associate trace file extensions with Wireshark*（将跟踪文件扩展名关联至 Wireshark）。单击 **Next** 继续。

图 2-5. Wireshark——附加任务



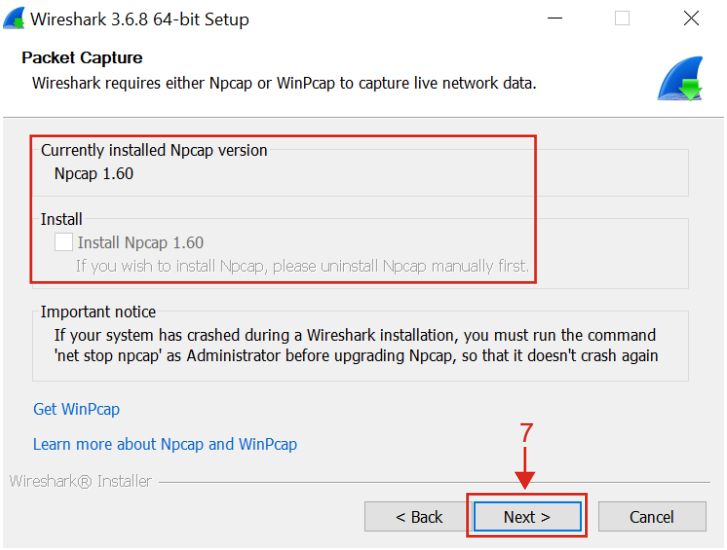
6. 将 Wireshark 安装到“Destination Folder”（目标文件夹）字段下的默认位置：*C:\Program Files\Wireshark*。单击 **Next** 继续。

图 2-6. Wireshark——安装位置



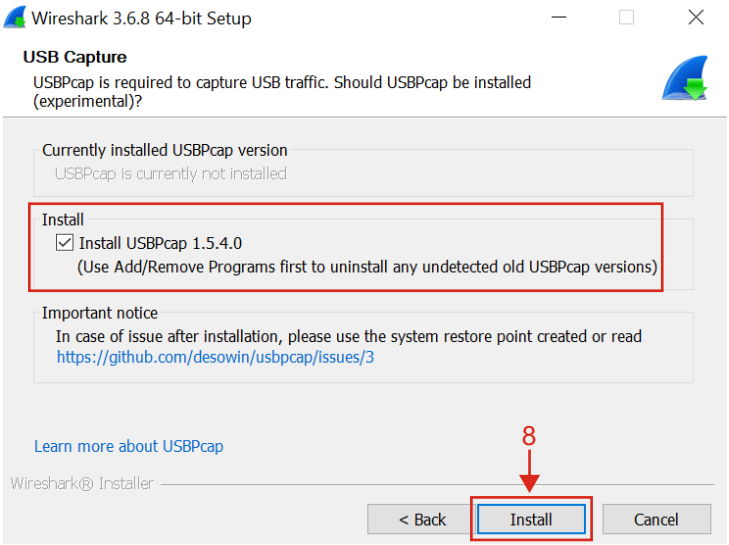
7. 安装“Npcap”或“WinPcap”以捕捉实时网络数据。在此场景中，安装的是 *Npcap 1.60*。单击 **Next** 继续。（可选）

图 2-7. Wireshark——数据包捕捉



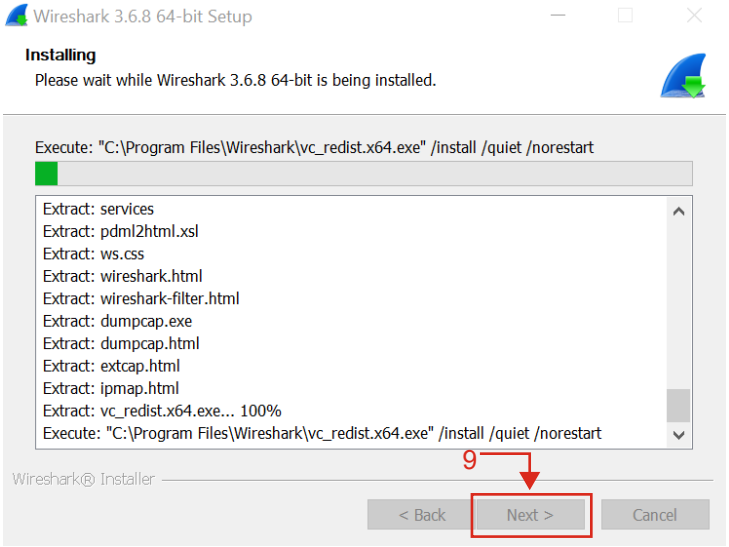
8. 安装“USBPcap”以捕捉 USB 流量。在此场景中，在“Install”（安装）字段下选中 *Install USBPcap 1.5.4.0*（安装 USBPcap 1.5.4.0）。单击 **Install** 继续。（可选）

图 2-8. Wireshark——USB 捕捉



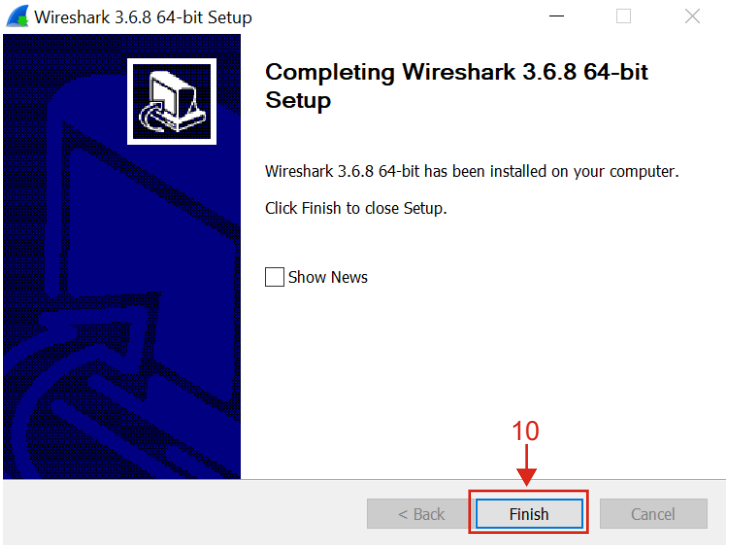
9. 用户必须等待 Wireshark 安装过程完成。安装过程完成后，单击 **Next** 继续。

图 2-9. Wireshark——正在安装



10. 单击 **Finish**（完成）以完成 Wirehsark 安装。

图 2-10. Wirehark 完成安装



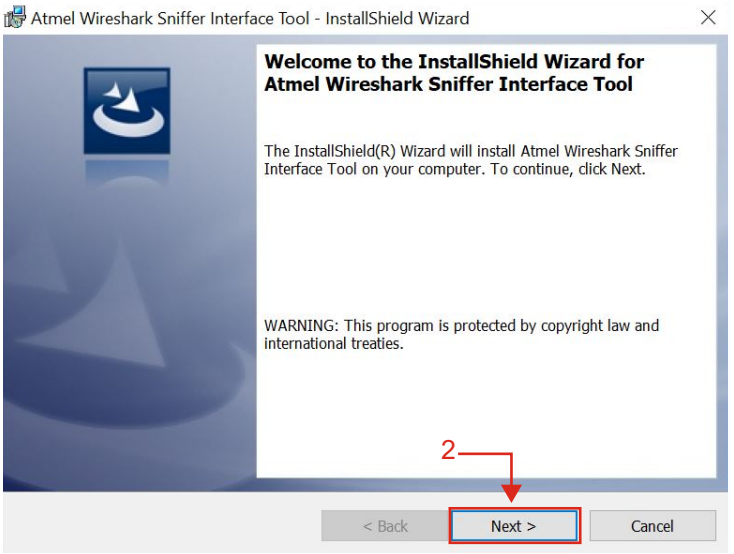
2.2.2. Wireshark Sniffer Interface Tool 安装

用户必须安装 Wireshark Sniffer Interface Tool 才能使用 Wireshark 设置捕捉会话。若要下载 Wireshark Sniffer Interface Tool，请访问 Wireshark Sniffer Interface Tool v3.0.0.10。

以下是安装 Wireshark Sniffer Interface Tool 的步骤：

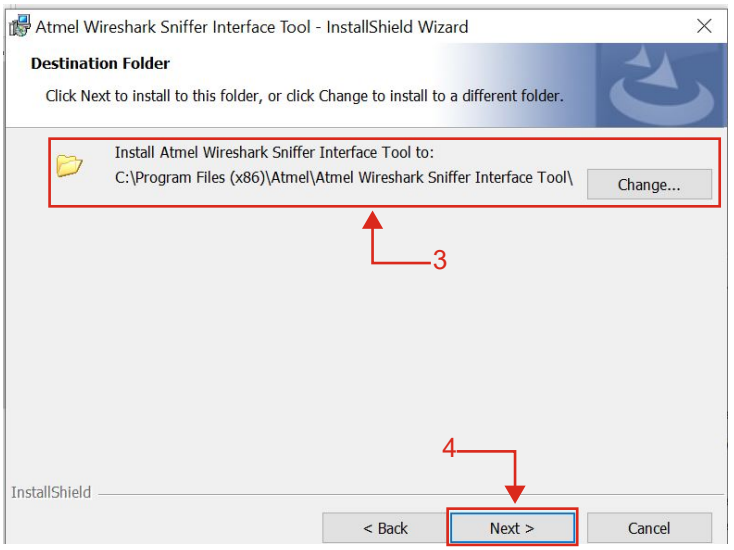
1. 双击 `Atmel Wireshark Sniffer Interface Tool.exe` 以启动安装过程。
2. 单击 **Next** 继续。

图 2-11. Wireshark Sniffer Interface Tool InstallShield 向导



3. 将 Wireshark Sniffer Interface Tool 安装到默认位置：*C:\Program Files (x86)\Atmel\Atmel Wireshark Sniffer Interface Tool\Atmel Wireshark Sniffer Firmware*。
4. 单击 **Next** 完成安装。

图 2-12. 默认位置——Wireshark Sniffer Tool 安装



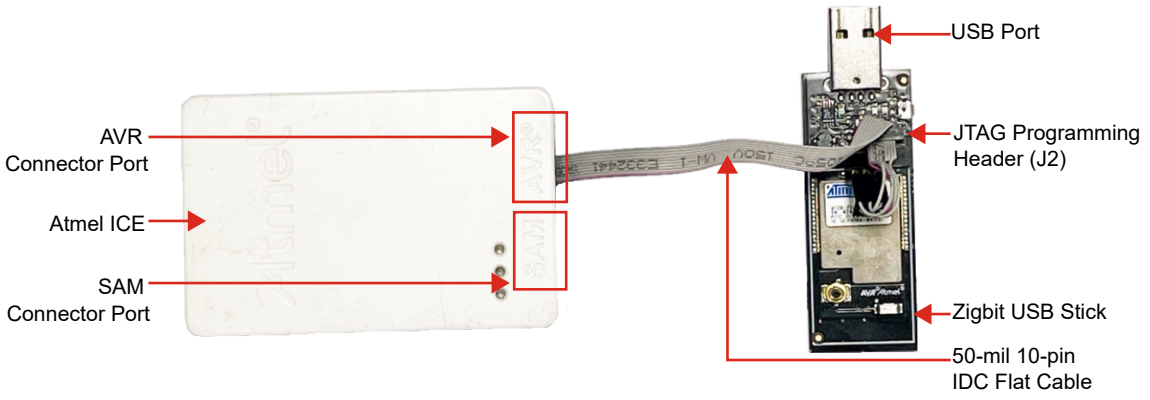
5. 按照 `Release Notes.txt`（位于软件包文件夹 `Atmel Wireshark Sniffer Interface Tool` 内）中的说明完成安装过程。有关详细信息，请参见 *ZigBit USB Stick User Guide*（42194）。
6. 在相应的 Zigbit 硬件平台上刷写嗅探器固件。有关详细信息，请参见将固件刷写到 ZigBit USB 设备中。以下是软件包中提供的映像：
   - `AWSI_at32uc3a3256s_rz600_at86rf212.hex`
   - `AWSI_at32uc3a3256s_rz600_at86rf231.hex`
   - `AWSI_atxmega256a3u_rf212b_zigbit_usb.hex`
   - `AWSI_atxmega256a3u_rf233_zigbit_usb.hex`

2.3. 将固件刷写到 ZigBit USB 设备中

以下是将固件刷写到 ZigBit USB 设备的步骤：

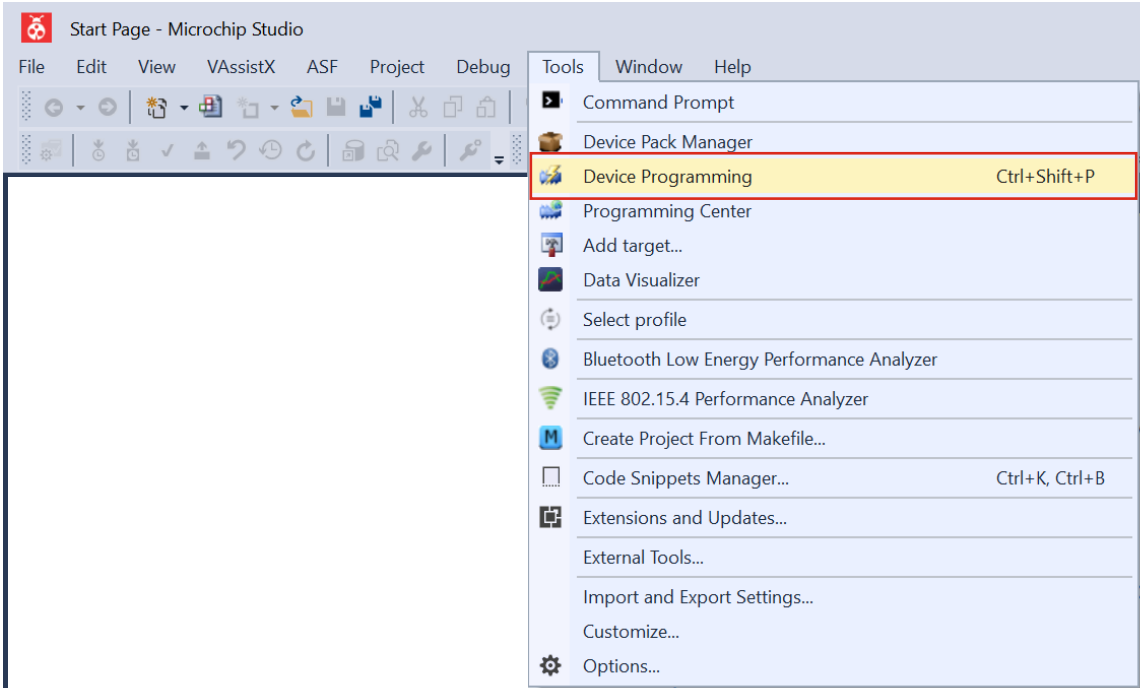
1. 使用 Atmel ICE JTAG 线缆连接 Atmel ICE 中的 AVR®连接器端口与 JTAG 编程连接器（J2）。有关详细信息，请参见 *ZigBit USB Stick User Guide*（42194）。
2. 使用 USB 线缆将 Atmel ICE 连接到 PC 的一个 COM 端口，并将 ZigBit USB 设备连接到 PC 的另一个 COM 端口。有关详细信息，请参见 *Atmel-ICE Programmers and Debuggers User Guide*（42330）。

图 2-13. Atmel ICE Zigbit 嗅探器连接



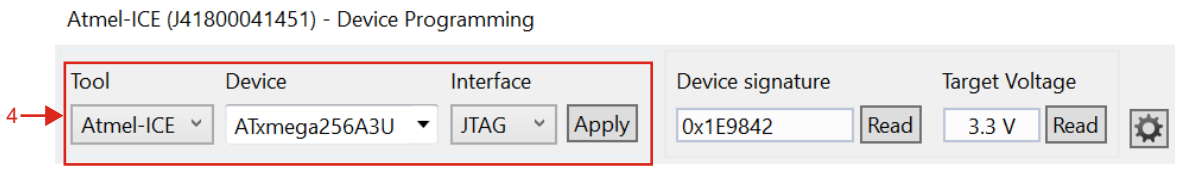
3. 打开 Microchip Studio，转到 *Tools* > *Device Programming*（工具 > 器件编程）并选择相应的工具、器件和接口。

图 2-14. 器件编程



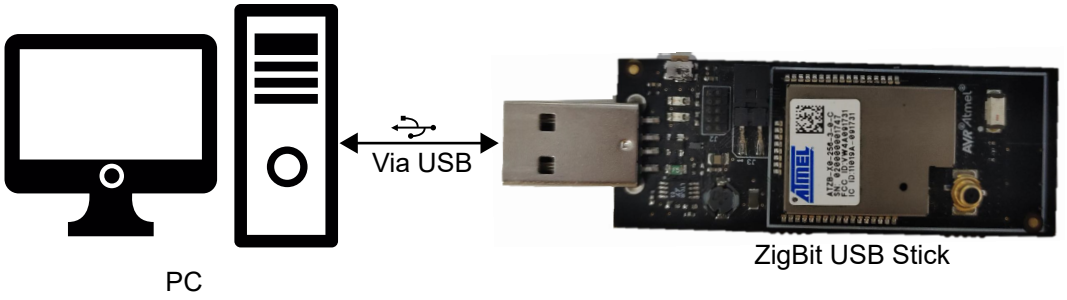
4. 用户必须选择以下字段：
   - 从“Tool”（工具）下拉列表中选择 *Atmel-ICE*。
   - 从“Device”（器件）下拉列表中选择 *ATxmega256A3U*。
   - 从“Interface”（接口）下拉列表中选择 *JTAG*。

图 2-15. 器件编程字段



5. 固件映像位于以下目录中：*\Atmel Wireshark Sniffer Interface Tool\Atmel Wireshark Sniffer Firmware*。从默认位置（步骤 3）加载 Wireshark 嗅探器固件，然后将固件刷写到 ZigBit 嗅探器中。
6. 断开 Atmel ICE 与 ZigBit USB 设备的连接。
7. 通过 USB 将 ZigBit USB 设备连接到 PC，然后打开 Atmel Wireshark Sniffer Interface Tool。

图 2-16. 将 ZigBee USB 设备连接到 PC



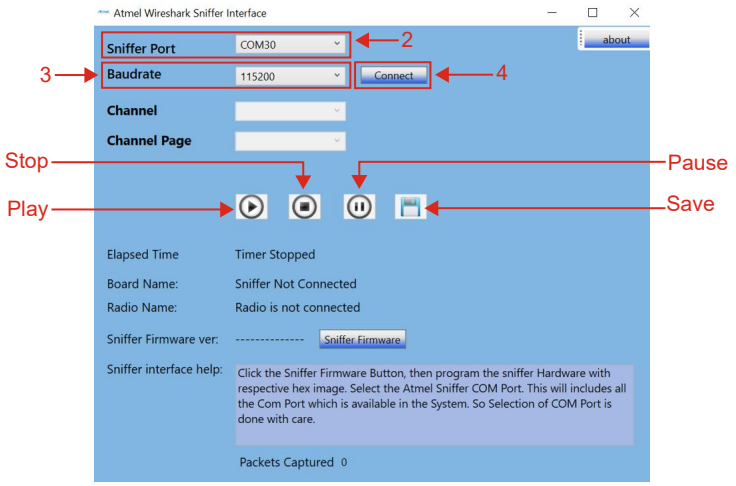
3. 嗅探器捕捉会话设置

本章提供有关在 PC 中成功安装 Wireshark Sniffer Interface Tool 后如何设置嗅探器捕捉会话的详细信息。

3.1. Wireshark 数据包捕捉步骤

1. 从开始菜单中单击 *Atmel Wireshark Sniffer Interface Tool* 以启动 Wireshark Sniffer Interface Tool。
2. 从“Sniffer Port”（嗅探器端口）下拉列表中选择 *COM30*（用于举例说明）。
3. 从“Baudrate”（波特率）下拉列表中选择 *115200*。
4. 单击 **Connect**（连接）继续。

图 3-1. Atmel Wireshark Sniffer Interface Tool 的启动窗口



5. 从“Channel”（信道）下拉列表中选择 *11*（用于举例说明）。
   注：用户可根据要求选择“Channel”。下面是可选值：
   - 对于 Sub-GHz，范围为 0-10。
   - 对于 2.4 GHz，范围为 11-26。
6. 从“Channel Page”（信道页）下拉列表中选择 *0*（用于举例说明）。可选值范围为 0-10。
   注：用户可根据定制数据速率要求调整“Channel Page”。
7. 单击 **Play**（开始）以开始捕捉。

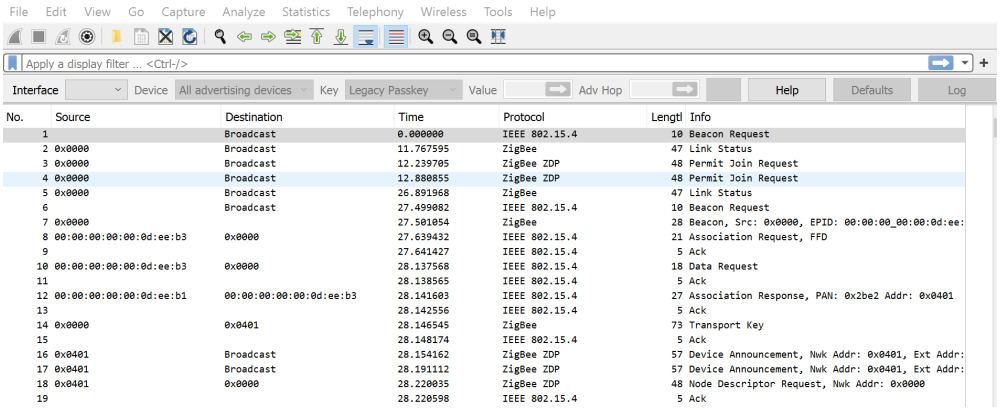
图 3-2. 信道/信道页/开始按钮

注：

- AT86RF233 ZIGBIT USB 设备（2.4 GHz）支持以下数据速率：
  - 信道页 0——数据速率为 250 kbps
  - 信道页 2——数据速率为 500 kbps
  - 信道页 16——数据速率为 1 Mbps
  - 信道页 17——数据速率为 2 Mbps
- AT86RF212B ZIGBIT USB 设备（Sub-GHz）支持以下数据速率：
  - 信道页 0——数据速率为 20 kbps（信道 0）和 40 kbps（信道 1-10）
  - 信道页 2——数据速率为 100 kbps（信道 0）和 250 kbps（信道 1-10）
  - 信道页 5——数据速率为 250 kbps
  - 信道页 16——数据速率为 200 kbps（信道 0）和 500 kbps（信道 1-10）
  - 信道页 17——数据速率为 400 kbps（信道 0）和 1 Mbps（信道 1-10）
  - 信道页 18——数据速率为 500 kbps
  - 信道页 19——数据速率为 1 Mbps

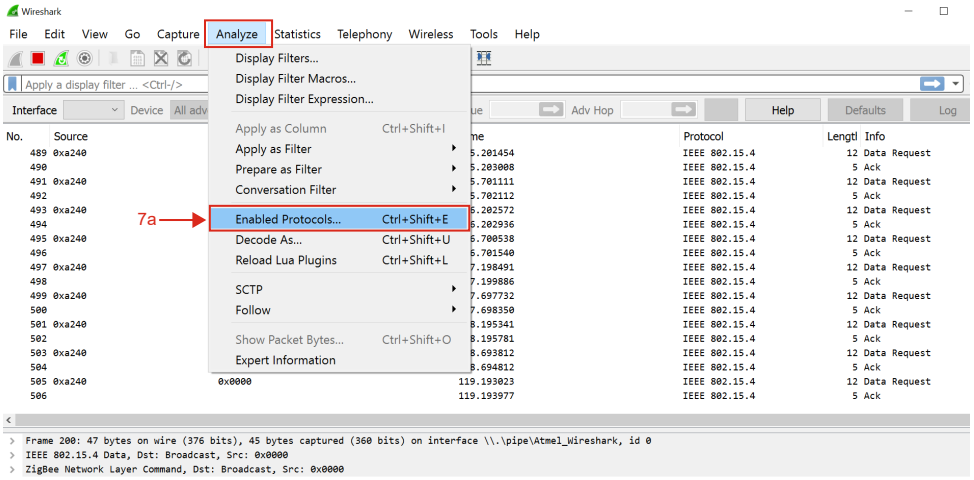
随后弹出以下窗口，其中显示在 Wireshark 中捕捉的数据包。

图 3-3. Wireshark 启动窗口



a. 转到 *Analyze* > *Enabled Protocols*（分析 > 已使能协议）以选择协议。

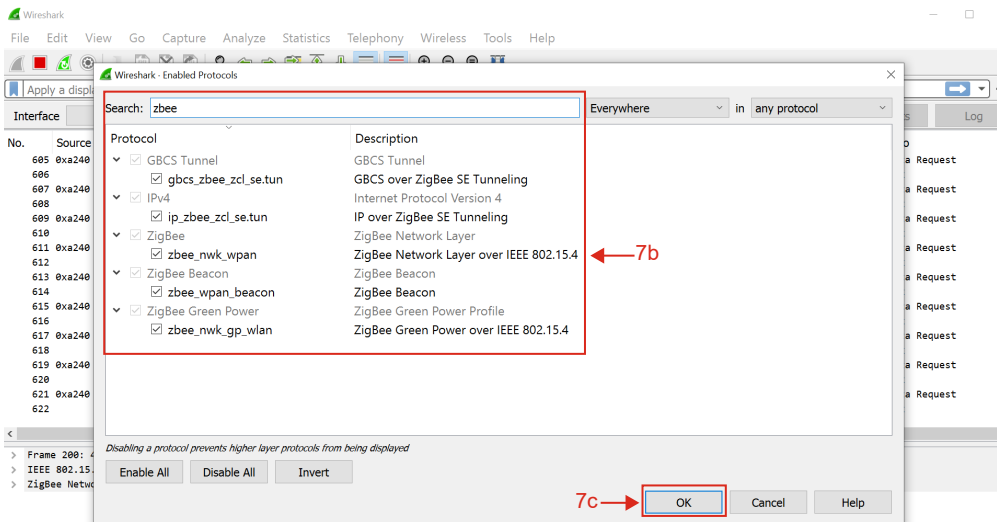
图 3-4. 已使能协议选择



b. 用户可根据要求选择协议。例如，在此场景中，搜索 *zbee* 以选择 **ZigBee** 协议。

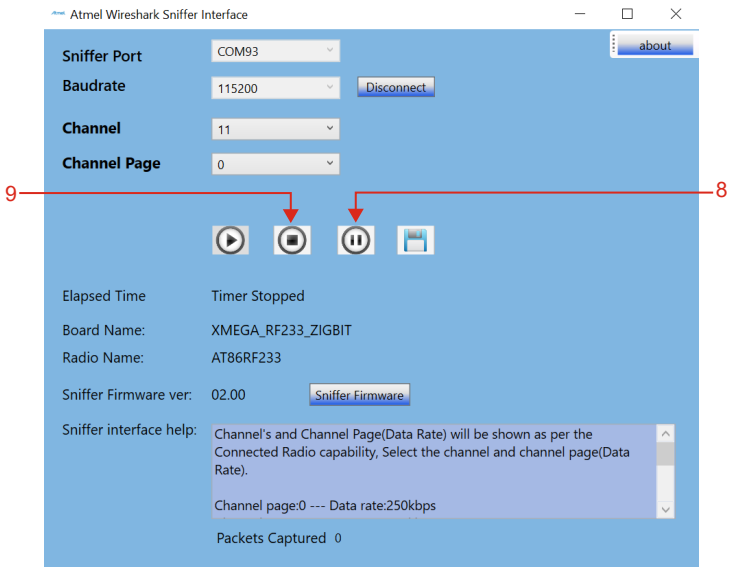
c. 单击 **OK**（确定）继续。

图 3-5. 协议选择



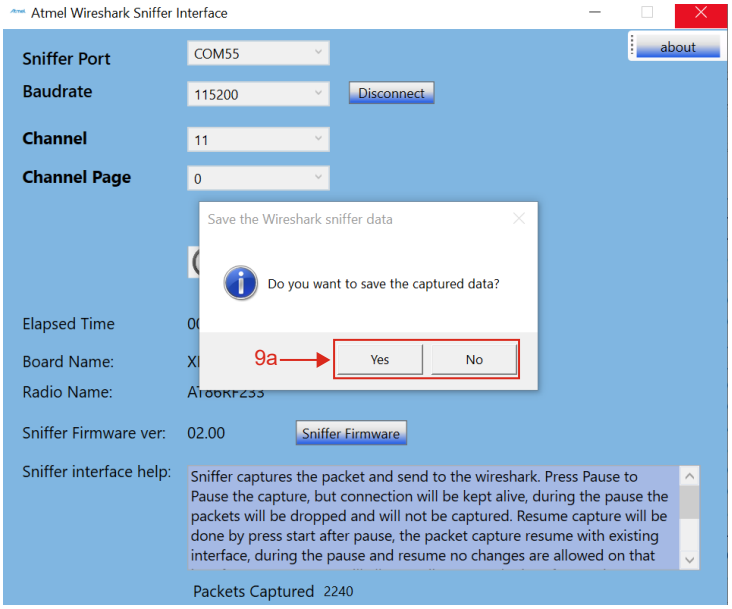
8. 单击 **Pause**（暂停）以暂停捕捉数据包。
9. 单击 **Stop**（停止）以停止捕捉数据包。

图 3-6. 暂停/停止按钮



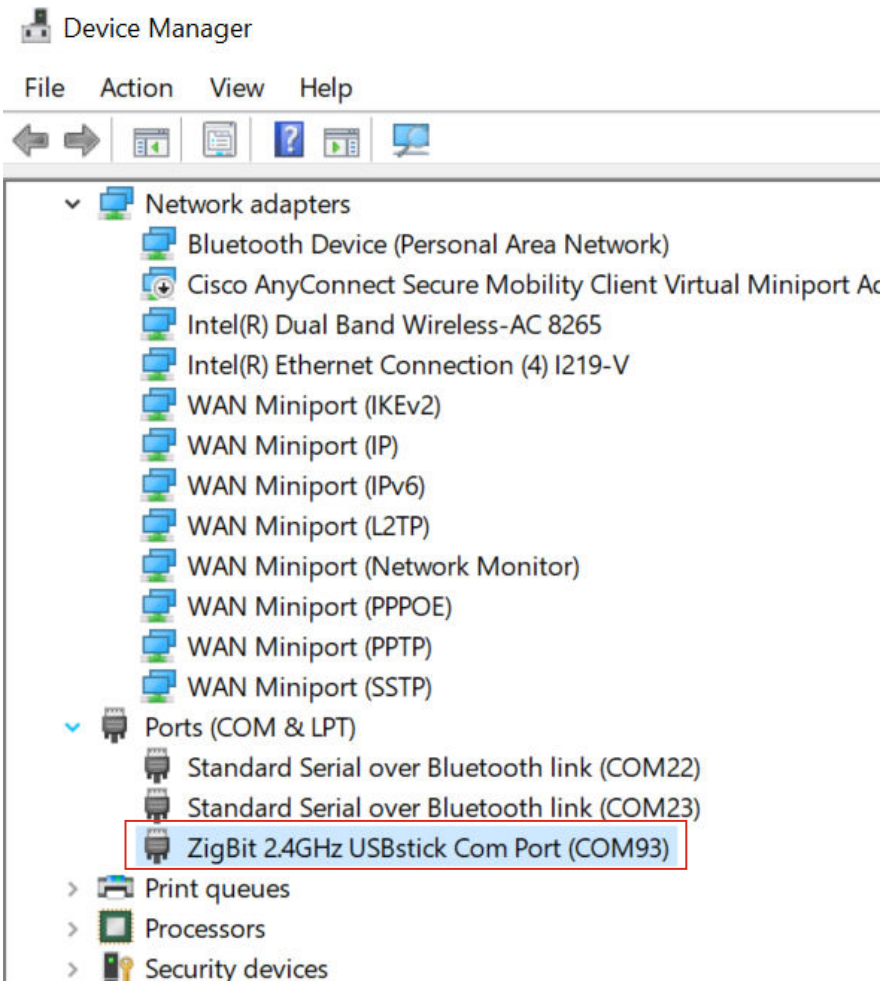
a. 随后弹出以下对话框，用户必须单击 **Yes**（是）或 **No**（否）以保存或删除捕捉文件（如果先前的信道/实例中有发生任何捕捉）。

图 3-7. 保存 Wireshark 嗅探器数据



10. 用户可保存捕捉的文件以供将来参考，也可在不保存的情况下继续。
    注：用户必须确保在系统环境变量中添加 `Wireshark-winXX-3.X.X.exe` 的路径。
11. 下图显示了 PC 的设备管理器中的 ZigBit 2.4 GHz USB 设备。

图 3-8. Windows 设备管理器中列出的 ZigBit 2.4 GHz USB 设备 COM 端口（嗅探器）



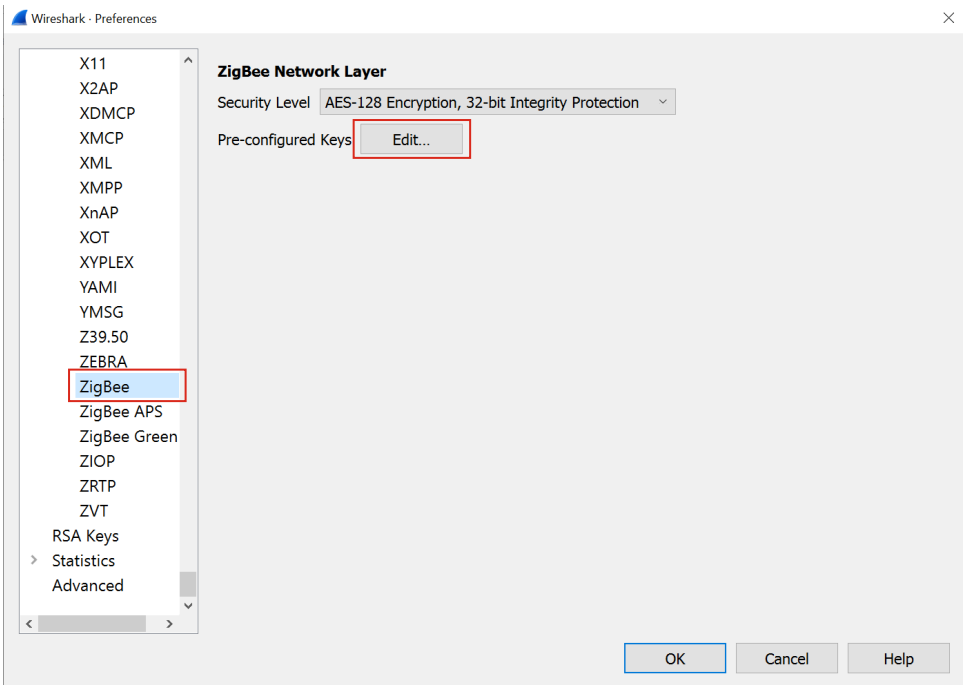
4. 配置嗅探器首选项

Wireshark 的 GUI 提供多种筛选选项，便于查看和分析。用户可通过适当的设置获得无线网络的完整概况。本章提供有关在 Wireshark 的 GUI 中配置此类首选项的信息。

4.1. Wireshark 捕捉界面

- 协议——Wireshark 自动识别正在使用的协议。默认情况下使能所有支持的协议，转到 *Analyze* > *Enabled Protocols* 可查看所有菜单选项。用户可使用该选项根据要求使能或禁止协议。
  注：用户必须确保在捕捉数据包之前使能全部所需的协议。
- 安全——可通过输入网络中使用的网络（NWK）安全密钥来监视加密的 ZigBee 网络数据。转到 *Edit* > *Preferences* > *Protocols* > *ZigBee*（编辑 > 首选项 > 协议 > ZigBee）。下图显示了 Wireshark 中的安全密钥配置选项。
  - 从“Pre-configured Keys”（预配置密钥）中单击 **Edit**（编辑）以输入安全密钥（见图 4-2）。

图 4-1. Wireshark 中的安全首选项



可根据 *Zigbee Specification Revision 22 1.0* 设置安全级别。下表提供了有关安全级别的详细信息。

表 4-1. NWK 和应用支持子层（APS）可用的安全级别

安全级别标识符	安全级别子字段	安全属性	数据加密	帧完整性（MIC 的长度 M，以八位字节数为单位）
0x00	000	无	关闭	否（M = 0）
0x01	001	MIC-32	关闭	是（M = 4）
0x02	010	MIC-64	关闭	是（M = 8）
0x03	011	MIC-128	关闭	是（M = 16）
0x04	100	ENC	ON	否（M = 0）
0x05	101	ENC-MIC-32	ON	是（M = 4）

表 4-1. NWK 和应用支持子层（APS）可用的安全级别 （续）

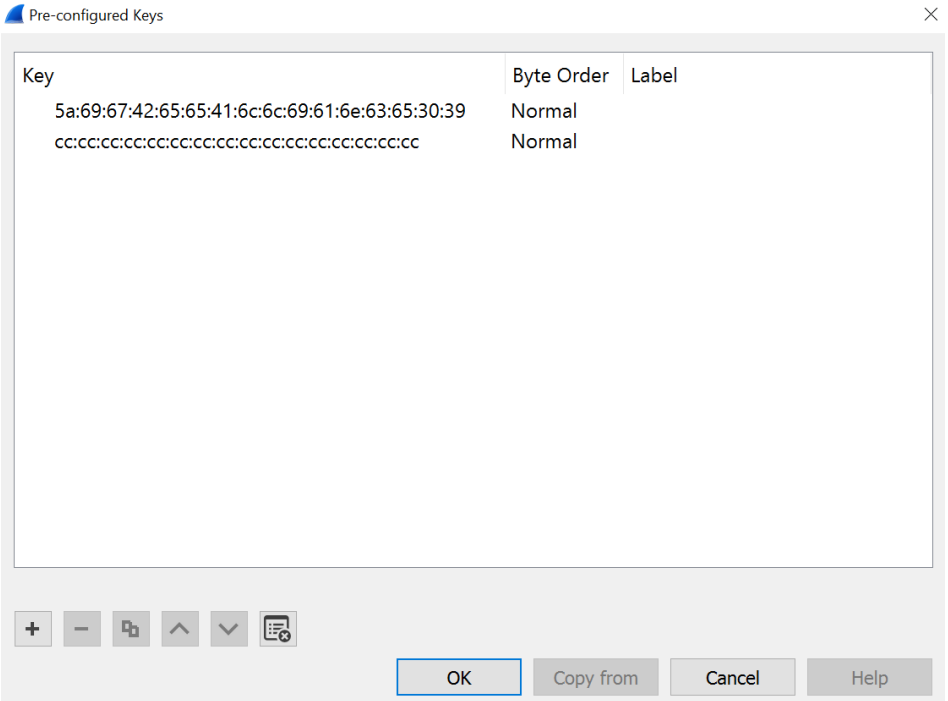
安全级别标识符	安全级别子字段	安全属性	数据加密	帧完整性（MIC 的长度 M，以八位字节数为单位）
0x06	110	ENC-MIC-64	ON	是（M = 8）
0x07	111	ENC-MIC-128	ON	是（M = 16）

注：有关安全级别的详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）中的 *Table 4-30 Security Levels Available to the NWK, and APS Layers*。

可添加多个密钥以及编辑或删除现有密钥。下图显示了安全密钥条目。

例如，对于在 APS 层使用集中式安全的 Zigbee 网络，加入网络的设备会与信任中心建立链路密钥。若要查看该链路中发生的所有 APS 事务（如 APS `Transport Key` 命令），请在 Wireshark 的首选项选项卡下添加信任中心链路密钥和网络密钥（见下图）。

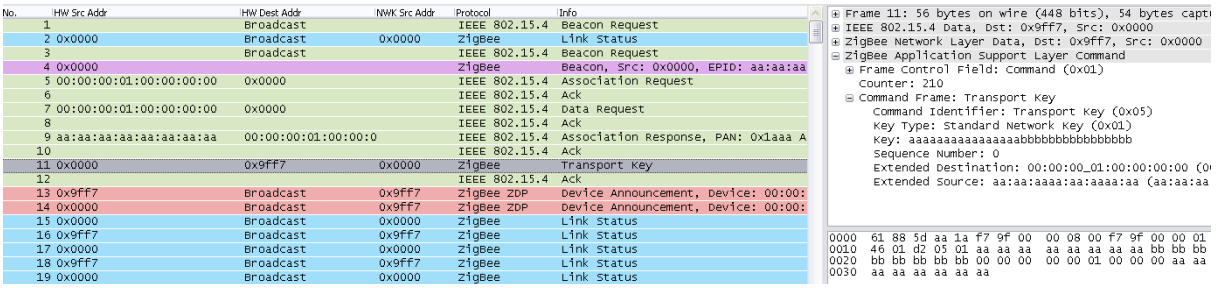
图 4-2. 安全密钥条目



用户可在 Wireshark 中自定义以下查看选项：

- 若要编排面板的布局，请转到 *Edit* > *Preferences* > *Layout*（编辑 > 首选项 > 布局）。
- 若要向数据包显示窗格中添加列（如 `HW Src Addr`），请转到 *Edit* > *Preferences* > *Columns*（编辑 > 首选项 > 列）。
- 若要对帧格式进行着色（如 NWK 链路状态帧），请转到 *View* > *Coloring Rules*（查看 > 着色规则）。有关详细信息，请参见 *Packet colorization*（11.3）。
- 按照以下步骤应用筛选器，以根据帧中所选的字段显示帧：
  a. 右键单击字段
  b. 选择 *Apply as Filter*（应用为筛选器）

图 4-3. Wireshark 捕捉屏幕布局



5. 分析 Zigbee Pro 网络中的数据流量

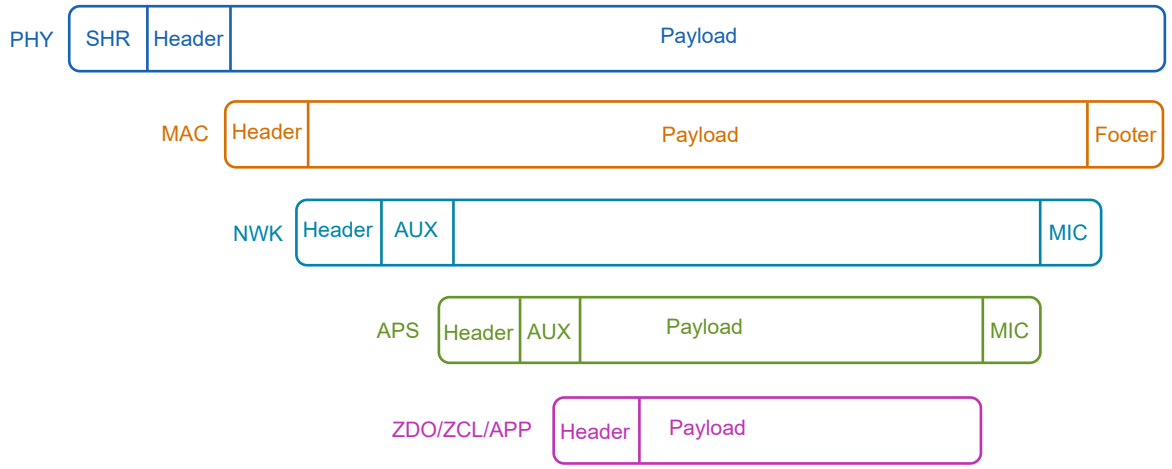
本章提供 Zigbee Pro 网络中的常见交互示例，帮助用户解析帧的各个字段。

注：本章内容并未涵盖 Zigbee 规范中的所有场景。

5.1. Zigbee 帧格式概述

下图给出了 Zigbee 帧格式的结构概览（包括 APS 和 NWK 层的安全帧头和帧尾）。Zigbee 使用一种非信标使能的 MAC 格式，MAC 层没有安全机制。

图 5-1. Zigbee 帧格式



5.2. MAC 关联

Zigbee 网络中的每个节点都有其惟一的 64 位 IEEE MAC 地址。当节点首次加入网络时，终端设备/路由器将发起 MAC 关联过程，之后将从父节点获取一个 16 位网络（短）地址。为降低帧开销，网络内的后续通信均使用该短地址。在编译期间，可使用配置参数“IEEE MAC 地址”设置该节点的 64 位 MAC 地址值。具体情况如下：

- 针对测试设置 `IEEE MAC address`——可在编译时通过应用程序配置文件设置任意随机的 64 位值，或者在运行时调用应用程序编程接口（API）启动网络请求之前通过 ZDP 进行设置。
- 在生产期间设置 `IEEE MAC address`——Zigbee 产品的商业用途需要从 IEEE 购买一个 IEEE/MAC 地址块。在这种情况下，可在编译期间将 `IEEE MAC address` 设置为零。

节点启动时，会通过在 Zigbee 协议栈参数配置文件或应用程序级别配置的信道列表中指定的信道上执行主动扫描来进行网络发现。节点发送 `Beacon Request`（见数据包#1）（见下图）。网络中已有的路由器和协调器收到 `Beacon Request` 帧后会自动以信标帧进行响应。入网节点根据收到的信标数据包中的设置来筛选潜在的父节点。

图 5-2. 节点使用 IEEE 地址 0xdeeb1ULL 通过 MAC 关联加入网络

No.	Source	Destination	Time	Protocol	Leng	Info
1		Broadcast	0.000000	IEEE 802.15.4	10	Beacon Request
2	0x0000	Broadcast	11.767595	ZigBee	47	Link Status
3	0x0000	Broadcast	12.239705	ZigBee ZDP	48	Permit Join Request
4	0x0000	Broadcast	12.880855	ZigBee ZDP	48	Permit Join Request
5	0x0000	Broadcast	26.891968	ZigBee	47	Link Status
6		Broadcast	27.499082	IEEE 802.15.4	10	Beacon Request
7	0x0000		27.501054	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
8	00:00:00:00:00:0d:ee:b3	0x0000	27.639432	IEEE 802.15.4	21	Association Request, FFD
9			27.641427	IEEE 802.15.4	5	Ack
10	00:00:00:00:00:0d:ee:b3	0x0000	28.137568	IEEE 802.15.4	18	Data Request
11			28.138565	IEEE 802.15.4	5	Ack
12	00:00:00:00:00:0d:ee:b1	00:00:00:00:00:0d:ee:b3	28.141603	IEEE 802.15.4	27	Association Response, PAN: 0x2be2 Addr: 0x0401
13			28.142556	IEEE 802.15.4	5	Ack

来自协调器/路由器的信标包含 `Association Permit` 子字段。如果该设备接受与个人局域网（Personal Area Network，PAN）的关联，则该子字段设置为 `True`。如果该子字段设置为 `False`，则入网节点无法与该设备关联。Zigbee 应用程序中的 `PERMIT DURATION` 参数通过设置有限的准入持续时间来控制设备加入网络。

图 5-3. 信标帧中的 assocPermit 子字段

```
IEEE 802.15.4 Beacon, Src: 0x0000
    <Frame Length: 26>
  > Frame Control Field: 0x8000, Frame Type: Beacon, Destination Addressing Mode: None, Frame Version: IEEE Std 802.15.4-2003, Source Addressing Mode: Short/16-bit
    Sequence Number: 249
    Source PAN: 0x1361
    Source: 0x0000
    <[Address: 0x0000]>
  v Superframe Specification: PAN Coordinator, Association Permit
        .... .... .... 1111 = Beacon Interval: 15
        .... .... 1111 .... = Superframe Interval: 15
        .... 1111 .... .... = Final CAP Slot: 15
        ...0 .... .... .... = Battery Extension: False
        .1.. .... .... .... = PAN Coordinator: True
        1... .... .... .... = Association Permit: True
  > GTS
    Pending Addresses: 0 Short and 0 Long
```

例如，下图显示了解析后的信标有效负载，其中包含的信息是入网节点选择潜在父节点的依据。

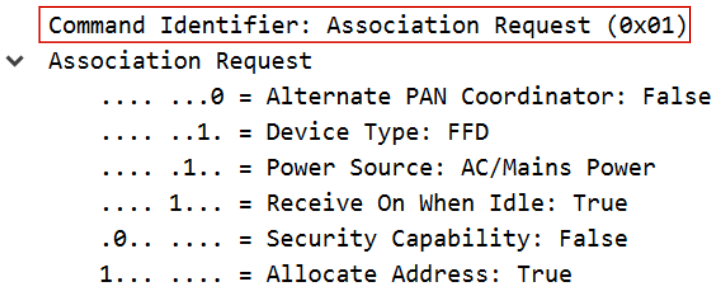
信标有效负载提供了网络中使用的 Zigbee 协议栈配置文件（`Stack Profile: ZigBee PRO = 0x2`）和网络协议版本（`nwkcProtocolVersion, 0x02`）信息。`Router Capacity`、`End Device Capacity` 和 `Device Depth` 会限制父节点对子节点的接受能力。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

图 5-4. 信标有效负载

```
ZigBee Beacon, ZigBee PRO, EPID: 00:00:00_00:00:00:0b:ee
    Protocol ID: 0
  v Beacon: Stack Profile: ZigBee PRO, Router Capacity, End Device Capacity
        .... .... .... 0010 = Stack Profile: ZigBee PRO (0x2)
        .... .... 0010 .... = Protocol Version: 2
        .... .1.. .... .... = Router Capacity: True
        .000 0... .... .... = Device Depth: 0
        1... .... .... .... = End Device Capacity: True
    Extended PAN ID: 00:00:00_00:00:00:0b:ee (00:00:00:00:00:00:0b:ee)
    Tx Offset: 16777215
    Update ID: 0
```

下图显示了入网设备在其发送给潜在父节点的 MAC Association Request 中所指示的自身能力信息。

图 5-5. MAC 关联请求中的能力信息



5.3. 自主离网和父节点触发离网

Zigbee 设备对象（ZDO）层负责管理 ZDP 请求，并将其用于各种网络控制场景。

如果设备需要在发生特定事件时离开网络，可使用 ZDP 请求来处理离网操作。离网可以由节点自身发起，也可以由一个节点指示另一个远程节点离开网络。

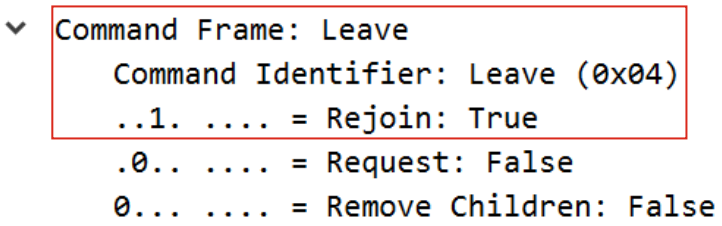
下图显示了短地址为 0x457a 的节点。该节点自主离开网络（自主触发），并通过发送重新加入请求来重新加入网络（见数据包#3300）。

图 5-6. 短地址为 0x457a 且扩展地址为 0xdeeb1ULL 的节点（终端设备）自主离网

3292	0x457a	Broadcast	868.566706	ZigBee	47	Leave
3293			868.567703	IEEE 802.15.4	5	Ack
3294		Broadcast	868.712432	IEEE 802.15.4	10	Beacon Request
3295	0x0000		868.715116	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
3296		Broadcast	869.131080	IEEE 802.15.4	10	Beacon Request
3297	0x0000		869.135077	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
3298		Broadcast	870.272629	IEEE 802.15.4	10	Beacon Request
3299	0x0000		870.275375	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
3300	0x457a	0x0000	870.694727	ZigBee	47	Rejoin Request, Device: 0x457a
3301			870.696141	IEEE 802.15.4	5	Ack
3302	0x457a	0x0000	871.271862	IEEE 802.15.4	12	Data Request
3303			871.272858	IEEE 802.15.4	5	Ack
3304	0x0000	0x457a	871.276892	ZigBee	57	Rejoin Response, New Address: 0x457a
3305			871.278842	IEEE 802.15.4	5	Ack

该节点之所以能重新入网是因为 Command Frame: Leave 中的 Rejoin 位设置为 True。下图显示了离网数据包的重新加入位设置。

图 5-7. 离网数据包的重新加入位设置



下图显示了父节点请求短地址为 0x6915 的子设备离网（Leave Request）（见数据包#99）的情况。子设备发送重新加入响应（见数据包#101）。几秒钟后，子设备使用相同的短地址重新加入网络。在这种情况下，子设备重新加入的是一个网络参数（如网络 PANID）已知的网络。

图 5-8. 父节点 0x0000 发送 ZDP 请求指示子节点 0x6915 离网

No.	Source	Destination	Time	Protocol	Leng	Info
99	0x0000	0x6915	344.198134	ZigBee ZDP	55	Leave Request, Device: 00:00:00_00:00:0d:ee:b3
100			344.199875	IEEE 802.15.4	5	Ack
101	0x6915	0x0000	344.200877	ZigBee ZDP	47	Leave Response, Status: Success
102			344.201874	IEEE 802.15.4	5	Ack
103	0x0000	0x6915	344.205547	ZigBee	45	APS: Ack, Dst Endpt: 0, Src Endpt: 0
104			344.207157	IEEE 802.15.4	5	Ack
105	0x6915	Broadcast	344.241797	ZigBee	47	Leave
106	0x6915	Broadcast	344.320390	ZigBee	47	Leave
107		Broadcast	344.324058	IEEE 802.15.4	10	Beacon Request
108	0x0000		344.327381	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b7
109	0x6915	0x0000	344.464216	ZigBee	47	Rejoin Request, Device: 0x6915
110			344.465868	IEEE 802.15.4	5	Ack
111	0x0000	0x6915	344.469117	ZigBee	57	Rejoin Response, New Address: 0x6915
112			344.469526	IEEE 802.15.4	5	Ack
113	0x6915	Broadcast	344.475399	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x6915, Ext Addr: 00:00:00_0
114	0x6915	Broadcast	344.550166	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x6915, Ext Addr: 00:00:00_0
115	0x6915	Broadcast	355.722891	ZigBee	50	Link Status
116	0x0000	Broadcast	356.902136	ZigBee	50	Link Status
117	0x6915	Broadcast	370.883667	ZigBee	50	Link Status

下图显示了父节点请求子设备离开网络且不重新加入的情况。

图 5-9. 不允许重新入网的父节点触发离网

No.	Source	Destination	Time	Protocol	Leng	Info
143	0x0000	0x6915	509.080714	ZigBee ZDP	55	Leave Request, Device: 00:00:00_00:00:0d:ee:b3
144			509.082196	IEEE 802.15.4	5	Ack
145	0x6915	0x0000	509.082196	ZigBee ZDP	47	Leave Response, Status: Success
146			509.083197	IEEE 802.15.4	5	Ack
147	0x0000	0x6915	509.086683	ZigBee	45	APS: Ack, Dst Endpt: 0, Src Endpt: 0
148			509.087212	IEEE 802.15.4	5	Ack
149	0x6915	Broadcast	509.163823	ZigBee	47	Leave
150	0x6915	Broadcast	509.245952	ZigBee	47	Leave
151	0x0000	Broadcast	523.198620	ZigBee	47	Link Status
152	0x0000	Broadcast	538.359397	ZigBee	47	Link Status
153	0x0000	Broadcast	553.399912	ZigBee	47	Link Status
154	0x0000	Broadcast	568.443126	ZigBee	47	Link Status
155	0x0000	Broadcast	583.525611	ZigBee	47	Link Status
156	0x0000	Broadcast	598.565007	ZigBee	47	Link Status
157		Broadcast	608.471662	IEEE 802.15.4	10	Beacon Request
158	0x0000		608.472570	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b7
159	00:00:00:00:00:0d:ee:b3	0x0000	609.032644	IEEE 802.15.4	21	Association Request, FFD
160			609.033977	IEEE 802.15.4	5	Ack
161	00:00:00:00:00:0d:ee:b3	0x0000	609.529476	IEEE 802.15.4	18	Data Request
162			609.530474	IEEE 802.15.4	5	Ack
163	00:00:00:00:00:0d:ee:b7	00:00:00:00:00:0d:ee:b3	609.533465	IEEE 802.15.4	27	Association Response, PAN: 0x0daf Addr: 0x0a18

图 5-8 与图 5-9 之间的区别在于重新加入位的设置。

- 如果重新加入位设置为 `True`，则离网设备使用重新加入请求来重新加入网络。
- 如果重新加入位设置为 `False`，在调用子设备加入网络的情况下，可通过 MAC 关联实现重新入网。

可在离网请求中配置子节点重新入网和移除等选项。

5.4. 网络（NWK）链路状态帧

路由器和协调器会发送网络（NWK）链路状态帧，以便相邻节点能够维护路由所需的链路成本信息。`Link Status` 帧会定期以单跳广播形式传输。`Link Status` 列表中包含所有相邻节点的短地址和链路成本信息。下图显示了 NWK 链路状态帧中的帧头信息。

图 5-10. NWK 链路状态命令帧

```
> Frame 144: 50 bytes on wire (400 bits), 48 bytes captured (384 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: Broadcast, Src: 0x0000
v ZigBee Network Layer Command, Dst: Broadcast, Src: 0x0000
  > Frame Control Field: 0x1209, Frame Type: Command, Discover Route: Suppress, Security, Extended Source Command
    Destination: 0xfffc
    <[Address: 0xfffc]>
    Source: 0x0000
    <[Address: 0x0000]>
    Radius: 1
    Sequence Number: 245
    Extended Source: 00:00:00_00:00:0d:ee:b1 (00:00:00:00:00:0d:ee:b1)
    <[Extended Address: 00:00:00_00:00:0d:ee:b1 (00:00:00:00:00:0d:ee:b1)]>
  > ZigBee Security Header
  v Command Frame: Link Status
      Command Identifier: Link Status (0x08)
      .1.. .... = Last Frame: True
      ..1. .... = First Frame: True
      ...0 0001 = Link Status Count: 1
    v Link 1
        Address: 0x0401
        .... .011 = Incoming Cost: 3
        .100 .... = Outgoing Cost: 4
```

5.5. 多播

向一组节点广播报文涉及到为指定的端点和组 ID 创建组表条目。下图显示了从协调器到组的多播传输，其中组 ID 为 `Group: 0x1111`，端点为 `0x20`。网络目标地址即为组地址。

图 5-11. 多播子字段——NWK 帧头

```
v ZigBee Application Support Layer Data, Group: 0x1111, Src Endpt: 20
  v Frame Control Field: Data (0x0c)
      .... ..00 = Frame Type: Data (0x0)
      .... 11.. = Delivery Mode: Group (0x3)
      ..0. .... = Security: False
      .0.. .... = Acknowledgement Request: False
      0... .... = Extended Header: False
    Group: 0x1111
    Cluster: On/Off (0x0006)
    Profile: Home Automation (0x0104)
    Source Endpoint: 20
    Counter: 26
v ZigBee Cluster Library Frame
  v Frame Control Field: Cluster-specific (0x11)
      .... ..01 = Frame Type: Cluster-specific (0x1)
      .... .0.. = Manufacturer Specific: False
      .... 0... = Direction: Client to Server
      ...1 .... = Disable Default Response: True
    Sequence Number: 13
    Command: On (0x01)
```

5.6. 分片

当应用层（APL）数据包的长度超过 APL 有效负载的最大限值时，协议栈会将整个数据分割成多个数据块。

图 5-12. 分片——相关帧头信息

```
> Frame 27: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
> IEEE 802.15.4 Data, Dst: 0xbc8f, Src: 0x0000
> ZigBee Network Layer Data, Dst: 0xbc8f, Src: 0x0000
v ZigBee Application Support Layer Data, Dst Endpt: 240, Src Endpt: 1
  v Frame Control Field: Data (0xc0)
      .... ..00 = Frame Type: Data (0x0)
      .... 00.. = Delivery Mode: Unicast (0x0)
      ..0. .... = Security: False
      .1.. .... = Acknowledgement Request: True
      1... .... = Extended Header: True
    Destination Endpoint: 240
    Cluster: Transmit Counted Packets (0x0001)
    Profile: Test Profile #2 (0x7f01)
    Source Endpoint: 1
    Counter: 160
  v Extended Frame Control Field (0x02)
      .... ..10 = Fragmentation: Middle Block (0x2)
      Block Number: 1
    Reassembled in: 43
v Data (30 bytes)
    Data: 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 …
    [Length: 30]
```

下图给出了一个分片示例。

图 5-13. 分片——示例

No.	Source	Destination	Time	Protocol	Length	Info
20	0xbc8f	Broadcast	21.493704	ZigBee ZDP	37	Device Announcement, Nwk Addr: 0xbc8f, Ext Addr: 00:00:00_02:00:00:00:00
21	0xbc8f	Broadcast	22.133464	ZigBee ZDP	37	Device Announcement, Nwk Addr: 0xbc8f, Ext Addr: 00:00:00_02:00:00:00:00
22	0x0000	Broadcast	25.155616	ZigBee	33	Link Status
23	0xcbff	Broadcast	29.473672	ZigBee	33	Link Status
24	0xbc8f	Broadcast	30.607360	ZigBee	33	Link Status
25	0x0000	0xbc8f	36.144840	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 0)
26			36.147112	IEEE 802.15.4	3	Ack
27	0x0000	0xbc8f	36.243768	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 1)
28			36.246048	IEEE 802.15.4	3	Ack
29	0x0000	0xbc8f	36.343496	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 2)
30			36.345768	IEEE 802.15.4	3	Ack
31	0xbc8f	0x0000	36.350384	ZigBee	28	APS: Ack, Dst Endpt: 1, Src Endpt: 240
32			36.351728	IEEE 802.15.4	3	Ack
33	0x0000	0xbc8f	36.355896	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 3)
34			36.358168	IEEE 802.15.4	103	Data
35	0x0000	0xbc8f	36.452296	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 4)
36			36.454568	IEEE 802.15.4	3	Ack
37	0x0000	0xbc8f	36.552688	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 5)
38			36.554960	IEEE 802.15.4	3	Ack
39	0xbc8f	0x0000	36.558864	ZigBee	28	APS: Ack, Dst Endpt: 1, Src Endpt: 240
40			36.560208	IEEE 802.15.4	3	Ack
41	0x0000	0xbc8f	36.564128	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1 (fragment 6)
42			36.566400	IEEE 802.15.4	3	Ack
43	0x0000	0xbc8f	36.662472	ZigBee T2	57	Transmit Counted Packets, Src Endpt: 1
44			36.664744	IEEE 802.15.4	3	Ack
45	0xbc8f	0x0000	36.670120	ZigBee	28	APS: Ack, Dst Endpt: 1, Src Endpt: 240
46			36.671464	IEEE 802.15.4	3	Ack

发送节点发送第一个分片时，其块编号等于组成整个 APL 数据的总块数。后续分片的块编号从 1 开始，直到最大传输窗口大小。接收节点在接收到传输窗口中的所有块后发送 APS 应答帧。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

5.7. 服务发现

服务发现是收集网络中其他设备所支持的簇信息的过程。服务发现会为每个支持的簇 ID 使用 ZDP 请求。服务发现请求可以是单播或广播，因此响应中会包含响应者的网络地址以及匹配的简单描述符信息。响应包含一个匹配列表，其中会列出支持所请求簇的端点。有关服务发现的详细信息，请参见分析 Zigbee 3.0 协议中的数据流量。

5.8. 安全网络中的隧道传输

考虑这样一种网络场景：某个节点通过路由器父节点以非安全方式入网，并且该入网节点在加入过程之前并不知道网络密钥。在这种情况下，使用 APS 命令将网络密钥从信任中心安全地传输到新加入的路由器，该命令称为 APS 隧道命令。

终端设备 0x0beeLL 通过数据包#89 加入路由器 0x3c08。父路由器会向信任中心发送 APS Update Device 命令（数据包#91），以通知其有节点加入或离开网络。下表和图 5-15 提供了有关设备更新状态的详细信息，信任中心据此采取必要的操作，即发送网络密钥或者移除该设备的密钥及相关安全计数器。

图 5-14. 隧道传输

No.	Source	Destination	Time	Protocol	Length	Info
82		Broadcast	415.660689	IEEE 802.15.4	8	Beacon Request
83	0x0000		415.662913	ZigBee	26	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b7
84	0x3c08		415.670713	ZigBee	26	Beacon, Src: 0x3c08, EPID: 00:00:00_00:00:0d:ee:b7
85	00:00:00:00:00:00:0b:ee	0x3c08	416.221401	IEEE 802.15.4	19	Association Request, FFD
86			416.222473	IEEE 802.15.4	3	Ack
87	00:00:00:00:00:00:0b:ee	0x3c08	416.719889	IEEE 802.15.4	16	Data Request
88			416.720865	IEEE 802.15.4	3	Ack
89	00:00:00:00:00:0d:ee:b3	00:00:00:00:00:00:0b:ee	416.722841	IEEE 802.15.4	25	Association Response, PAN: 0x40a8 Addr: 0x54d7
90			416.724105	IEEE 802.15.4	3	Ack
91	0x3c08	0x0000	416.726233	ZigBee	66	Update Device
92			416.728801	IEEE 802.15.4	3	Ack
93	0x0000	0x3c08	416.732801	ZigBee	100	Transport Key
94			416.736465	IEEE 802.15.4	3	Ack
95	0x3c08	0x54d7	416.737593	ZigBee	71	Transport Key
96			416.740329	IEEE 802.15.4	3	Ack
97	0x54d7	Broadcast	416.745681	ZigBee ZDP	55	Device Announcement, Nwk Addr: 0x54d7, Ext Addr: 00:00:00_00:00
98	0x54d7	Broadcast	416.781937	ZigBee ZDP	55	Device Announcement, Nwk Addr: 0x54d7, Ext Addr: 00:00:00_00:00

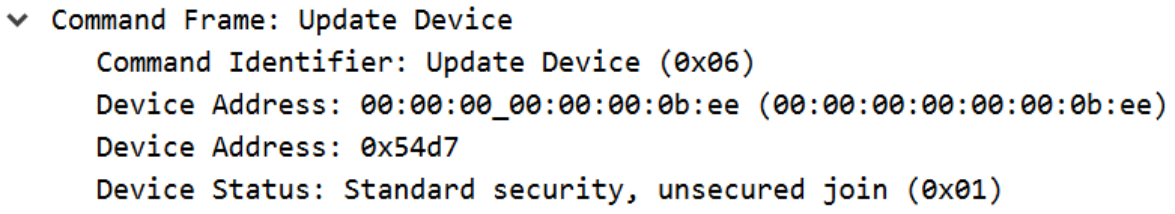
信任中心在数据包#93 中发送 APS 隧道命令帧。该隧道命令帧的有效负载中包含要发送到目标的安全帧。数据包#95 显示了从路由器父节点发送到新加入的终端设备的 APS Transport Key 命令帧，其中包含密钥序列号和有效网络密钥。如果路由器使用预配置的网络密钥加入，则尽管 APS 传输数据包中包含密钥序列号，但密钥值为全零。终端设备接收 Transport Key 命令帧，设置并激活网络密钥，然后向网络发出设备通告（数据包#97 和#98）。

表 5-1. APS 更新设备命令中的状态字段

参数名称	类型	有效范围	说明
状态	整数	0x00-0x07	指示由 DeviceAddress 参数指定的设备的更新状态。 • 0x00 = 标准设备以安全方式重新入网 • 0x01 = 标准设备以非安全方式入网 • 0x02 = 设备离网 • 0x03 = 标准设备以非安全方式重新入网 • 0x04 = 高安全性设备以安全方式重新入网 • 0x05 = 高安全性设备以非安全方式入网 • 0x06 = 保留 • 0x07 = 高安全性设备以非安全方式重新入网

注： 有关 APS 更新设备命令中状态字段的详细信息，请参见 *ZigBee Specification Revision 22 1.0*（05-3474-22）。

图 5-15. 更新设备状态



6. 分析 Zigbee 3.0 协议中的数据流量

Zigbee 联盟定义了一组标准设备类型。这些设备类型规定了设备的功能。该功能又依赖于称为簇的独立功能实体。簇是属性的容器，可通过 Zigbee 设备配置文件（ZDP）定义的命令/响应进行读/写。该联盟还提供了 Zigbee 簇库（ZCL），作为簇功能的资源库。

本次数据包捕捉使用 Wireshark/Zigbit 嗅探器执行，针对的是多种 Zigbee 设备类型组合之间的数据传输。以下是三种 Zigbee 设备类型：

- Zigbee 协调器/Zigbee 组合接口——能够控制和监视其他设备的设备。通常为市电供电设备，例如个人计算机。
- Zigbee 路由器/Zigbee 灯具——可以打开/关闭的照明设备。可通过颜色命令调整灯光的亮度和颜色。
- Zigbee 终端设备/Zigbee 多传感器

以下是两种 Zigbee 网络架构：

- 集中式网络——Zigbee 协调器设备可以组建集中式网络。
- 分布式网络——Zigbee 路由器设备可以组建分布式网络。

数据包捕捉侧重于以下场景：

- Zigbee 协调器——集中式网络组建（Zigbee 组合接口应用）。Zigbee 协调器与 Zigbee 路由器（Zigbee 扩展彩色灯）之间的调试和数据交换。有关详细信息，请参见 Zigbee 协调器。
- Zigbee 路由器——扩展灯具应用被调试接入由 Zigbee 协调器组建的现有 Zigbee 网络（组合接口或 Zigbee 路由器能够组建新的 Zigbee 分布式网络（如果附近没有网络））。在此场景中，它被调试接入由 Zigbee 协调器/组合接口组建的现有 Zigbee 集中式网络。有关详细信息，请参见 Zigbee 路由器。
- Zigbee 终端设备——加入 Zigbee 协调器（组合接口）。加入后，终端设备（多传感器/传感器设备类型）在连接到由协调器组建的网络后开始报告传感器数据（如温度、占用状态、光照和湿度）的 ZCL 属性。有关详细信息，请参见 Zigbee 终端设备。
- Touchlink 调试——在本应用笔记中，调试过程发生在 Zigbee 扩展灯具（路由器）与彩色场景控制器（终端设备）之间。有关详细信息，请参见 Touchlink 调试。

6.1. 概述

6.1.1. 基础设备行为（BDB）

BDB（基础设备行为）层支持运行在 Zigbee PRO 协议栈上的基础设备的初始化、调试和操作过程，以确保配置文件互操作性。有关详细信息，请参见 *PRO Base Device Behavior Specification*（3.0.1）。

调试

调试是初始化设备以加入网络并协同工作的过程。Zigbee BDB 规范规定了以下调试机制的执行顺序：

1. Touchlink——节点可支持基于接近度的调试机制。如果支持 touchlink 调试，则节点支持作为发起方、目标方或两者的 touchlink。
   - 发起方——现有网络的成员，或者（如果不是）创建一个新网络
   - 目标方——由发起方添加到网络
2. 网络引导——所有节点均支持网络引导。
   - 未加入网络的节点——搜索并加入一个开放网络的行为
   - 已加入网络的节点——开放网络以允许新节点加入的行为
3. 网络组建——节点以其网络安全模型组建网络的能力。这取决于节点的逻辑设备类型。
   - Zigbee 协调器——组建集中式安全网络
   - Zigbee 路由器——组建分布式安全网络

4. 查找和绑定——以下是查找和绑定中的两个过程：
   - 发起方端点——通过使用识别簇与匹配簇，自动搜索并与目标端点建立应用层连接。
   - 目标方端点——处理来自发起方端点的查找和绑定请求

6.1.2. 网络安全模型

Zigbee 网络可支持集中式安全模型（集中式安全网络）或分布式安全模型（分布式安全网络）。除 Zigbee 协调器外的所有设备都能够加入支持任一模型的网络，或适应其所加入网络的安全条件。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

集中式安全网络

集中式安全网络是由具备信任中心功能的 Zigbee 协调器组建的 Zigbee 网络。信任中心会对每个加入此类网络的节点进行身份验证，通过身份验证的节点才能在网络上运行。创建集中式网络后，Zigbee 协调器设备不得尝试加入其他网络。

默认全局信任中心链路密钥

所有设备均支持的链路密钥，用于在没有其他特定链路的情况下加入集中式安全网络。
在集中式网络中，使用以下密钥允许设备入网。

- 全局信任中心链路密钥——可使用该链路密钥加入集中式安全网络。该密钥的值为 `0x5a 0x69 0x67 0x42 0x65 0x65 0x41 0x6c 0x6c 0x69 0x61 0x6e 0x63 0x65 0x30 0x39`。
- 安装码链路密钥——从入网设备的安装码派生出的链路密钥，用于创建入网时使用的惟一信任中心链路密钥。

分布式安全网络

分布式安全网络是由 Zigbee 路由器组建的 Zigbee 网络，不具备信任中心功能。父节点会对每个加入此类网络的节点进行身份验证，通过身份验证的节点才能在网络上运行。被指定为 Zigbee 路由器逻辑设备类型的节点可尝试加入现有的集中式或分布式安全网络。不过，Zigbee 路由器不能组建集中式安全网络，但可以组建分布式安全网络。被指定为 Zigbee 终端设备逻辑设备类型的节点可尝试加入现有的集中式或分布式安全网络。

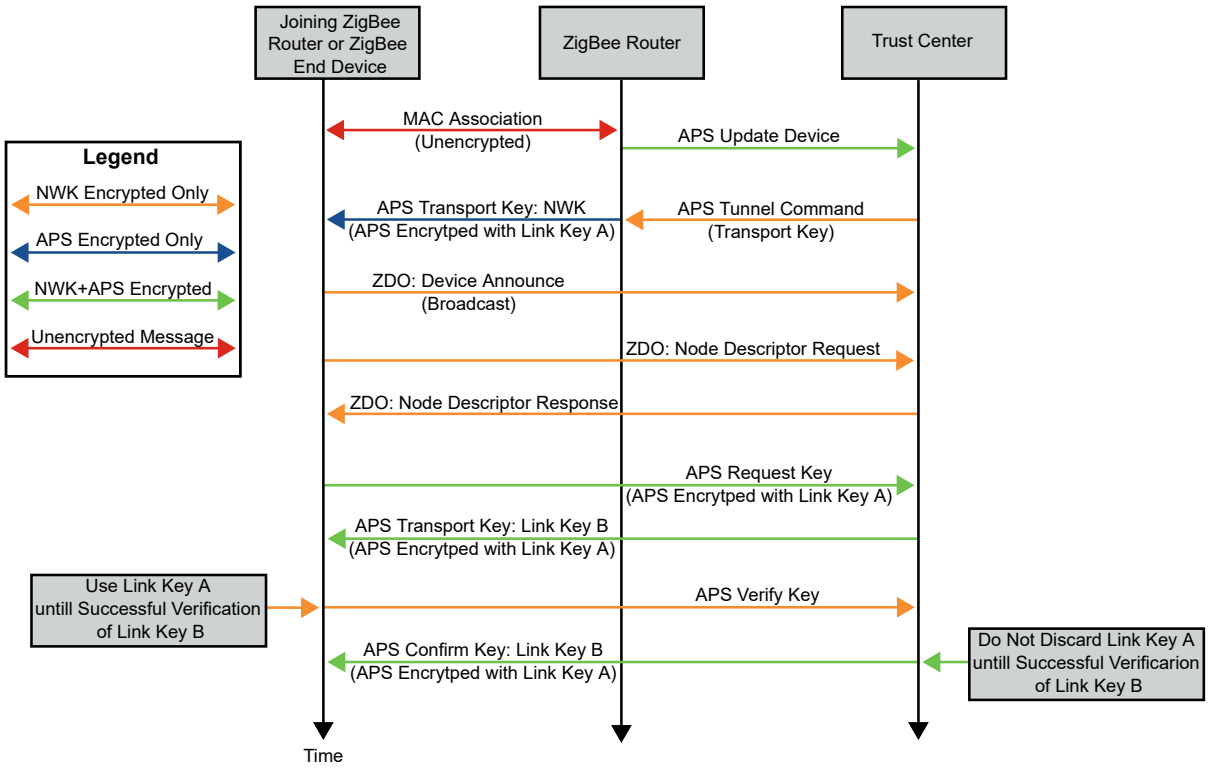
APL 层安全

- `Transport Key` 服务——支持以安全方式将密钥传输到其他设备。通过安全传输密钥命令，可将链路密钥或网络密钥从密钥源（如信任中心）传输到其他设备。
- `Request Key` 服务——支持设备以安全方式从信任中心请求端到端应用链路密钥或信任中心链路密钥。
- `Verify Key` 服务——支持设备以安全方式验证自身与信任中心是否就设备链路密钥的当前值达成一致。
- `Confirm Key` 服务——支持信任中心以安全方式确认先前的验证链路密钥请求。

有关详细信息，请参见 *PRO Base Device Behavior Specification*（3.0.1）。

信任中心链路密钥交换过程

图 6-1. 信任中心链路密钥交换过程序列图



有关详细信息，请参见 *PRO Base Device Behavior Specification*（3.0.1）。

6.1.3. Zigbee 设备配置文件（ZDP）

设备发现

设备发现机制使设备能够发现 PAN 上其他设备的身份。64 位 IEEE 地址和 16 位网络地址均支持设备发现。

- 设备通告——使网络上的 Zigbee 设备能够通知其他 Zigbee 设备该设备已加入或重新加入网络。此外，还有助于识别设备的 64 位 IEEE 地址和新的 16 位 NWK 地址，并向远程设备通告该 Zigbee 设备的能力。该原语的目标地址广播给所有 `macRxOnWhenIdle = True` 的设备。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

服务发现

设备使用服务发现过程来发现其他设备的能力，或识别支持类似服务（簇）的其他设备。服务发现后，设备将知晓支持相同簇的设备的端点和地址。为完成该过程，需对给定设备上的每个端点发出查询，或使用匹配服务功能（广播或单播）。服务发现机制定义并利用各种描述符来概述设备的能力。服务发现在 Zigbee 设备对象内实现。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

服务发现是 Zigbee 网络中的设备识别支持类似服务（簇）的其他设备的过程。服务发现后，设备将知晓支持相同簇的设备的端点和地址。

- 节点描述符——包含有关 Zigbee 节点能力的信息。本地设备通过发起服务发现机制来获取远程设备的节点描述符。该数据包能够以单播形式传输到远程设备本身或包含远程设备发现信息的其他设备。
- 简单描述符——允许查询设备获取所提供端点的簇详细信息。该数据包支持单播。

6.1.4. Zigbee 簇库规范（ZCL）

属性报告

报告簇的属性是指使用特定的 ZCL 属性报告命令将特定簇属性的值返回到支持该簇的远程端点。

属性报告在设备成功加入 Zigbee 网络并完成服务发现后开始。服务发现后，设备将知晓与其支持相同簇的设备的端点和地址。充当服务器簇的设备可向支持相同簇的客户端发送周期性报告。

有关详细信息，请参见 *ZigBee Alliance Cluster Library Specification Revision 8*（075123）。

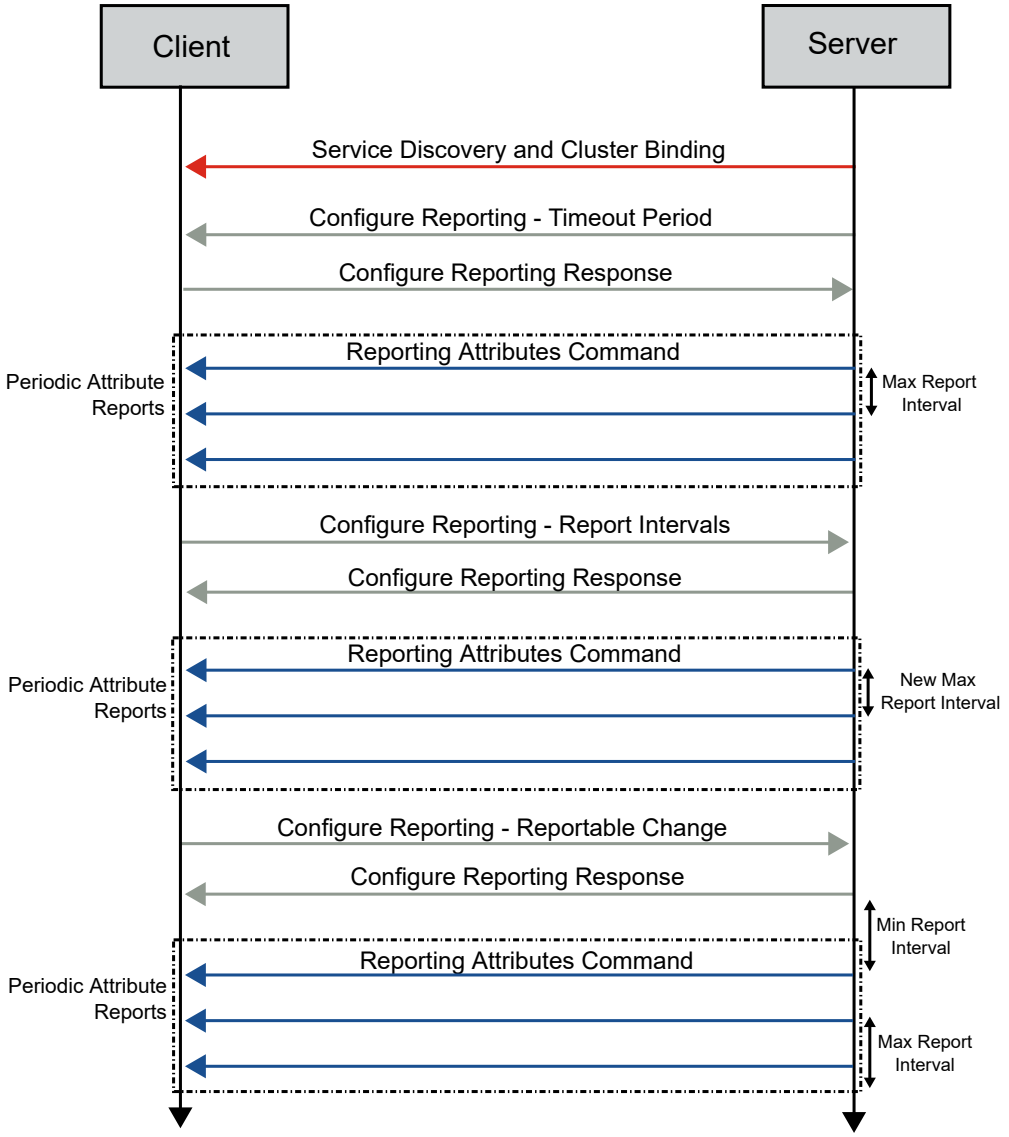
周期性报告

周期性报告有以下类型：

- 自动报告——用户可在编译时或运行时从应用程序配置簇的报告间隔。Zigbee 协议栈应用程序在每个最大报告间隔周期发送一次周期性报告。
- 基于属性值变化进行报告。
- 手动报告——应用程序可随时通过 ZCL 层使用属性请求发出报告。

有关详细信息，请参见 *AT08550: ZigBee Attribute Reporting Application Note*（42334）。

图 6-2. 属性报告——典型数据包交换序列



6.2. Zigbee 协调器

在 Zigbee 集中式网络中，由 Zigbee 协调器组建网络。其他路由器和终端设备可在网络组建后加入。

以下章节详细阐述了 Zigbee 协调器设备类型（与 Zigbee 路由器）的关联、调试、查找和绑定、属性报告以及安全密钥交换过程。

6.2.1. 调试

6.2.1.1. Zigbee 协调器/组合接口的集中式网络组建和网络引导

下图显示了网络地址为 `0x0000` 的 Zigbee 协调器/组合接口设备组建网络以及允许其他设备加入网络的网络引导场景。

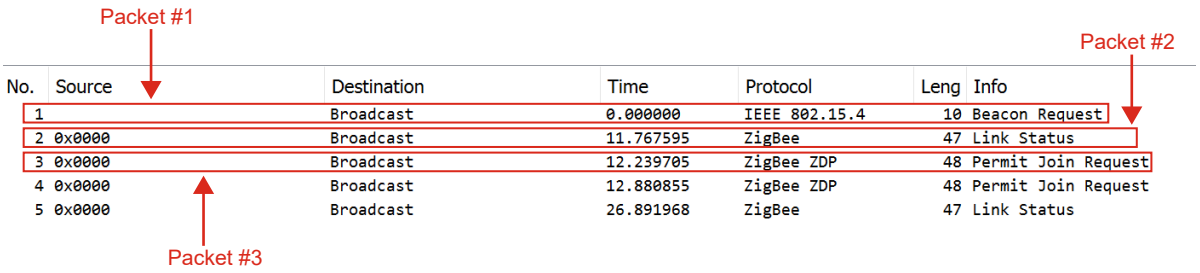
在调用网络组建调试过程后，协调器发送 `Beacon Request` 数据包（见数据包#1），随后进行 MAC 关联过程。有关详细信息，请参见 MAC 关联。

协调器组建网络后，将发送 Link Status（见数据包#2）。有关详细信息，请参见网络（NWK）链路状态帧。

允许入网 ZDP 请求旨在通过 MAC 关联为目标节点提供入网许可。该请求既可作为单播命令仅发送给一个节点，也可作为广播命令进行发送。根据有效负载的 Permit Duration 字段，允许在给定的秒数间隔内通过 MAC 关联入网或永久禁止入网。该字段指定从接收到请求的时刻起，允许通过关联入网的持续时间。

数据包#3 显示了 Permit Join Request，协调器设备以广播数据包形式发送该请求。有关详细信息，请参见 MAC 关联。

图 6-3. ZigBee 协调器的网络组建和网络引导

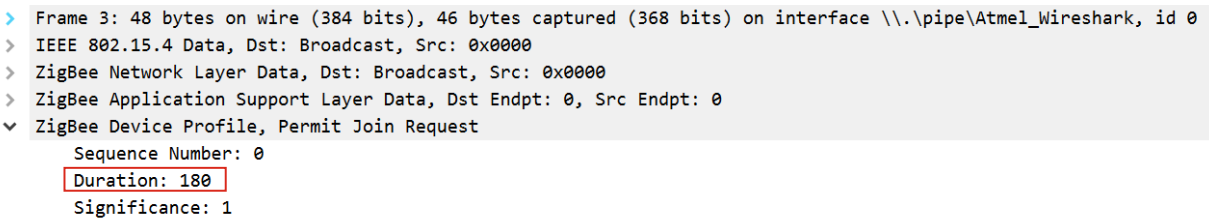


准入持续时间数据包的准入持续时间为 Duration: 180。路由器/终端设备必须在 180 秒内通过 MAC 关联加入网络。

若要在 180 秒后开放网络并允许其他设备加入，用户必须在其他设备启动调试之前向协调器输入以下命令：

- setPermitJoin 180——在接下来的 180 秒内开放网络
- invokeCommissioning 8 0——为查找和绑定过程开放网络

图 6-4. 协调器的允许入网数据包



MAC 关联——如果任何路由器/终端设备尝试通过 Beacon Request 加入网络，协调器会发送 Beacon 帧（见数据包#7）。然后，设备通过 MAC Association Request 加入网络，协调器以 Association Response（见数据包#12）进行响应。下图显示了 MAC 关联——协调器。有关详细信息，请参见 MAC 关联。

图 6-5. MAC 关联——协调器

No.	Source	Destination	Time	Protocol	Leng	Info
3	0x0000	Broadcast	12.239705	ZigBee ZDP	48	Permit Join Request
4	0x0000	Broadcast	12.880855	ZigBee ZDP	48	Permit Join Request
5	0x0000	Broadcast	26.891968	ZigBee	47	Link Status
6		Broadcast	27.499082	IEEE 802.15.4	10	Beacon Request
7	0x0000		27.501054	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
8	00:00:00:00:00:0d:ee:b3	0x0000	27.639432	IEEE 802.15.4	21	Association Request, FFD
9			27.641427	IEEE 802.15.4	5	Ack
10	00:00:00:00:00:0d:ee:b3	0x0000	28.137568	IEEE 802.15.4	18	Data Request
11			28.138565	IEEE 802.15.4	5	Ack
12	00:00:00:00:00:0d:ee:b1	00:00:00:00:00:0d:ee:b3	28.141603	IEEE 802.15.4	27	Association Response, PAN: 0x2be2 Addr: 0x0401
13			28.142556	IEEE 802.15.4	5	Ack

6.2.2. 服务发现

节点描述符——路由器/终端设备在查找和绑定之前的初始化过程中请求节点描述符。有关节点描述符的详细信息，请参见 Zigbee 设备配置文件（ZDP）。

- 数据包#18——显示了来自路由器节点的 Node Descriptor Request
- 数据包#20——显示了来自协调器节点的 Node Descriptor Response

图 6-6. 节点描述符

No.	Source	Destination	Time	Protocol	Leng	Info
18	0x0401	0x0000	28.220035	ZigBee ZDP	48	Node Descriptor Request, Nwk Addr: 0x0000
19			28.220598	IEEE 802.15.4	5	Ack
20	0x0000	0x0401	28.223487	ZigBee ZDP	62	Node Descriptor Response, Rev: 22, Nwk Addr: 0x0000, Status: Success
21			28.225483	IEEE 802.15.4	5	Ack
22	0x0401	0x0000	28.226481	ZigBee	45	APS: Ack, Dst Endpt: 0, Src Endpt: 0

下图显示了来自协调器设备的 Node Descriptor Response，用户可在 ZigBee Device Profile 下看到协调器节点的以下信息：

- Capability Information
- Max Buffer Size
- Server Flags
- Descriptor Capability Field

图 6-7. 节点描述符响应

```
> Frame 20: 62 bytes on wire (496 bits), 60 bytes captured (480 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x0401, Src: 0x0000
> ZigBee Network Layer Data, Dst: 0x0401, Src: 0x0000
> ZigBee Application Support Layer Data, Dst Endpt: 0, Src Endpt: 0
v ZigBee Device Profile, Node Descriptor Response, Rev: 22, Nwk Addr: 0x0000, Status: Success
    Sequence Number: 1
    Status: Success (0)
    Nwk Addr of Interest: 0x0000
  v Node Descriptor
      .... .... .... .000 = Type: 0 (Coordinator)
      .... .... .... 0... = Complex Descriptor: False
      .... .... ...1 .... = User Descriptor: True
      .... 0... .... .... = 868MHz BPSK Band: False
      ..0. .... .... .... = 902MHz BPSK Band: False
      .1.. .... .... .... = 2.4GHz OQPSK Band: True
      0... .... .... .... = EU Sub-GHz FSK Band: False
    > Capability Information: 0x0f
      Manufacturer Code: 0x1014
      Max Buffer Size: 71
      Max Incoming Transfer Size: 43
    > Server Flags: 0x2c40
      Max Outgoing Transfer Size: 43
    > Descriptor Capability Field: 0x00
```

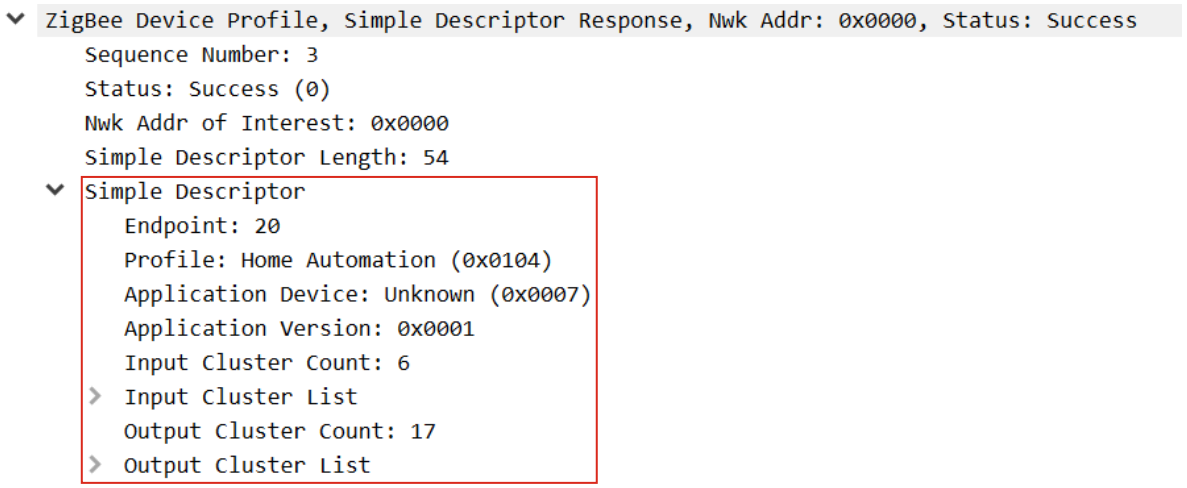
简单描述符——从协调器接收到 `Identify Query Response` 后，路由器识别目标方端点并向目标方端点（协调器）发送简单描述符请求。数据包#53 和#55 分别是来自路由器和协调器设备的 `Simple Descriptor Request` 和 `Simple Descriptor Response`。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

图 6-8. 简单描述符——协调器和路由器

No.	Source	Destination	Time	Protocol	Length	Info
47	0x3c08	Broadcast	270.393782	ZigBee HA	46	ZCL Identify: Identify Query, Seq: 0
48	0x0000	0x3c08	270.399198	ZigBee HA	48	ZCL Identify: Identify Query Response, Seq: 0
49			270.401198	IEEE 802.15.4	3	Ack
50	0x3c08	0x0000	270.403622	ZigBee	43	APS: Ack, Dst Endpt: 20, Src Endpt: 35
51			270.405470	IEEE 802.15.4	3	Ack
52	0x3c08	Broadcast	270.436398	ZigBee HA	46	ZCL Identify: Identify Query, Seq: 0
53	0x3c08	0x0000	270.442286	ZigBee ZDP	47	Simple Descriptor Request, Nwk Addr: 0x0000, Endpoint: 20
54			270.444253	IEEE 802.15.4	3	Ack
55	0x0000	0x3c08	270.446654	ZigBee ZDP	102	Simple Descriptor Response, Nwk Addr: 0x0000, Status: Success
56			270.450381	IEEE 802.15.4	3	Ack
57	0x3c08	0x0000	270.453318	ZigBee	43	APS: Ack, Dst Endpt: 0, Src Endpt: 0
58			270.455157	IEEE 802.15.4	3	Ack

下图显示了来自协调器的 `Simple Descriptor Response`，其中列出了其支持的输入和输出簇。

图 6-9. 简单描述符响应



6.2.3. 查找和绑定

配置为目标方端点和发起方端点的设备如下：

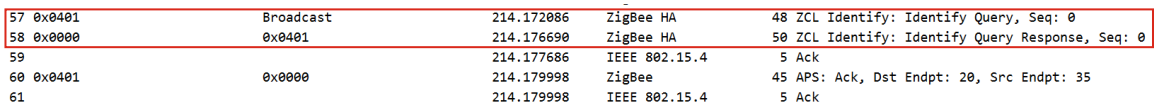
- 目标方端点——Zigbee 协调器/组合接口
- 发起方端点——Zigbee 路由器/扩展灯具

作为目标方端点的协调器接收来自路由器的 Identify Query 请求，协调器向发起方端点（路由器）发送 Identify Query Response。

下图显示数据包#57 和#58 分别是来自路由器和协调器设备的 Identify Query 请求和 Identify Query Response。

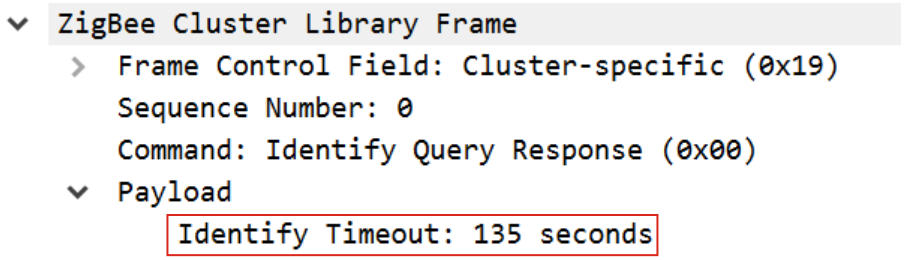
目标方端点在有限持续时间内标识自身，然后处理来自发起方端点的后续查找和绑定请求。

图 6-10. 标识查询



下图显示了目标方端点的 Identify Timeout: 135 seconds。

图 6-11. 标识超时



当标识超时属性递减至零时，目标设备将终止针对目标方端点的查找和绑定过程。

6.2.4. 报告

作为客户端的设备能够发起设备发现、服务发现、绑定或网络管理请求。作为服务器的设备为这些请求提供服务并予以响应。客户端和服务器角色并非互斥，一个给定的设备可同时充当客户端和服务器。

设备配置文件以如下两种配置之一来描述设备：

- 客户端——通过设备配置文件报文向服务器发出请求
- 服务器——向发起设备配置文件报文的客户端发出响应

下表提供了 Microchip Zigbee 协议栈中组合接口设备类型可用的客户端/服务器簇的详细信息。有关详细信息，请参见 *ZigBee Alliance Cluster Library Specification Revision 8*（075123）。有关特定设备类型的强制或可选簇的详细信息，请参见 *Matter Device Library Specification*（1.0）。

注：组合接口设备类型仅在 Microchip Zigbee 协议栈中受支持。

表 6-1. 支持的簇——组合接口

设备类型	服务器簇 ID	服务器簇	客户端簇 ID	客户端簇
组合接口	0x0000	基本	0x0000	基本
	0x0003	识别	0x0003	识别
	0x0004	组	0x0004	组
	0x000A	时间	0x0005	场景
	0x0501	IAS ACE	0x0006	开/关
	0x0008	级别控制	0x0009	报警
	0x0300	颜色控制	0x0201	温控器
	—	—	0x0202	风扇控制
	—	—	0x0406	占用检测
	—	—	0x0400	照度测量
	—	—	0x0402	温度测量
	—	—	0x0204	温控器 UI
	—	—	0x0405	含水量测量
	—	—	0x0500	IAS 区域

在此场景中，协调器/组合接口配置为目标方端点；因此，协调器设备不报告任何属性。该设备监视由路由器/终端设备报告的属性。

6.2.5. 安全

地址为 0x0000 的 Zigbee 协调器/组合接口设备充当信任中心，地址为 0x0401 的设备充当 Zigbee 路由器（见下图）。有关集中式安全机制的详细信息，请参见网络安全模型。

根据图 6-1，MAC 关联数据包未加密。关联过程完成后：

1. 信任中心发送 Transport Key（地址为 0x0000 的协调器），入网设备从中接收链路密钥（路由器——0x0401）（见数据包#14）。承载传输密钥的 APS 帧使用链路密钥 A 进行加密。
2. 入网设备（路由器）执行设备通告（见数据包#16 和#17）。
3. 协调器与路由器在初始化过程中交换节点描述符（见数据包#18 到#22）。
4. 数据包#23 显示路由器向信任中心发送请求密钥，以请求链路 Key B。链路 Key A 保护承载该请求密钥的 APS 帧。
5. 信任中心通过 Transport Key 传输（数据包#25）所请求的密钥，并由链路 Key A 进行 APS 加密。
6. 数据包#27 显示了 Verify Key，确保信任中心和入网设备就同一密钥达成一致。

7. 数据包#29 显示了 Confirm Key，允许信任中心确认先前的验证链路密钥请求。

图 6-12. 集中式网络中的信任中心密钥交换

	No.	Source	Destination	Time	Protocol	Leng	Info
	6		Broadcast	27.499082	IEEE 802.15.4	10	Beacon Request
	7	0x0000		27.501054	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
	8	00:00:00:00:00:0d:ee:b3	0x0000	27.639432	IEEE 802.15.4	21	Association Request, FFD
	9			27.641427	IEEE 802.15.4	5	Ack
	10	00:00:00:00:00:0d:ee:b3	0x0000	28.137568	IEEE 802.15.4	18	Data Request
	11			28.138565	IEEE 802.15.4	5	Ack
	12	00:00:00:00:00:0d:ee:b1	00:00:00:00:00:0d:…	28.141603	IEEE 802.15.4	27	Association Response, PAN: 0x2be2 Addr: 0x0401
	13			28.142556	IEEE 802.15.4	5	Ack
1	14	0x0000	0x0401	28.146545	ZigBee	73	Transport Key
	15			28.148174	IEEE 802.15.4	5	Ack
2	16	0x0401	Broadcast	28.154162	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x0401, Ext Addr: 00:00:00_00:00:0d:ee:b3
	17	0x0401	Broadcast	28.191112	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x0401, Ext Addr: 00:00:00_00:00:0d:ee:b3
	18	0x0401	0x0000	28.220035	ZigBee ZDP	48	Node Descriptor Request, Nwk Addr: 0x0000
	19			28.220598	IEEE 802.15.4	5	Ack
3	20	0x0000	0x0401	28.223487	ZigBee ZDP	62	Node Descriptor Response, Rev: 22, Nwk Addr: 0x0000, Status: Success
	21			28.225483	IEEE 802.15.4	5	Ack
	22	0x0401	0x0000	28.226481	ZigBee	45	APS: Ack, Dst Endpt: 0, Src Endpt: 0
4	23	0x0401	0x0000	28.230471	ZigBee	66	Request Key
	24			28.232511	IEEE 802.15.4	5	Ack
5	25	0x0000	0x0401	28.237494	ZigBee	90	Transport Key
	26			28.239448	IEEE 802.15.4	5	Ack
6	27	0x0401	0x0000	28.242440	ZigBee	65	Verify Key
	28			28.244433	IEEE 802.15.4	5	Ack
7	29	0x0000	0x0401	28.247426	ZigBee	67	Confirm Key, SUCCESS
	30			28.249421	IEEE 802.15.4	5	Ack

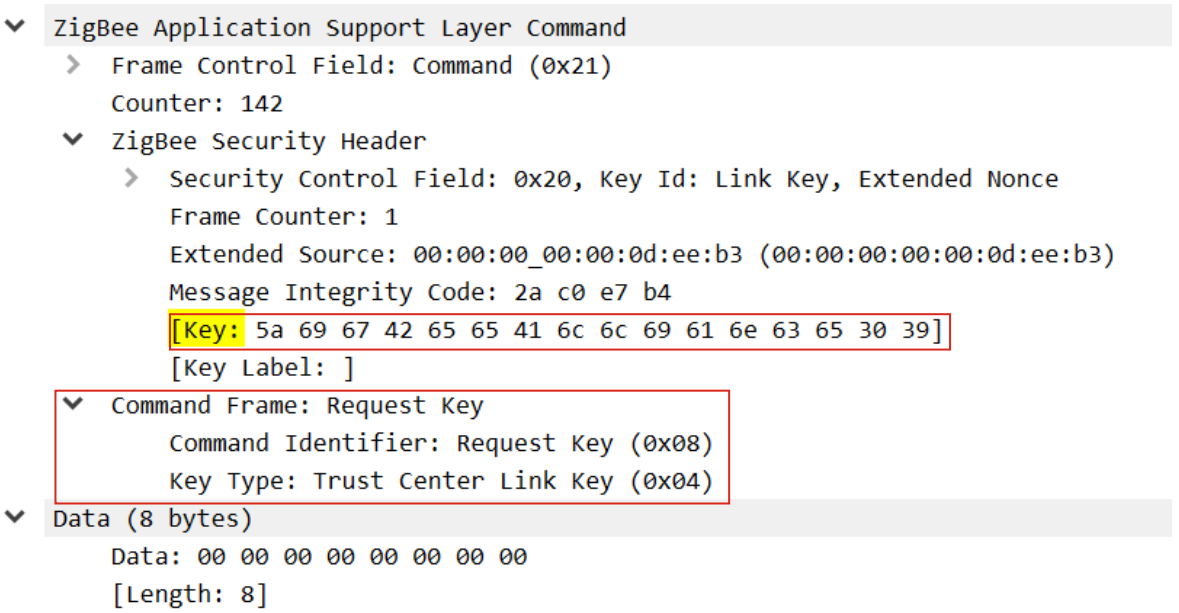
下图显示了 Transport Key，其中高亮显示了用于加密 APS 层的链路 Key A（5a 69 67 42 65 65 41 6c 6c 69 61 6e 63 65 30 39）。默认情况下，网络密钥用于簇命令。下图高亮显示了网络密钥 Key: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc。

图 6-13. APS 隧道传输密钥

```
▼ ZigBee Application Support Layer Command
  ▶ Frame Control Field: Command (0x21)
    Counter: 203
  ▼ ZigBee Security Header
    ▶ Security Control Field: 0x30, Key Id: Key-Transport Key, Extended Nonce
      Frame Counter: 1
      Extended Source: 00:00:00_00:00:0d:ee:b1 (00:00:00:00:00:0d:ee:b1)
      Message Integrity Code: 22 47 99 22
      [Key: 5a 69 67 42 65 65 41 6c 6c 69 61 6e 63 65 30 39]
      [Key Label: ]
  ▼ Command Frame: Transport Key
      Command Identifier: Transport Key (0x05)
      Key Type: Standard Network Key (0x01)
      Key: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
      Sequence Number: 0
      Extended Destination: 00:00:00_00:00:0d:ee:b3 (00:00:00:00:00:0d:ee:b3)
      Extended Source: 00:00:00_00:00:0d:ee:b1 (00:00:00:00:00:0d:ee:b1)
```

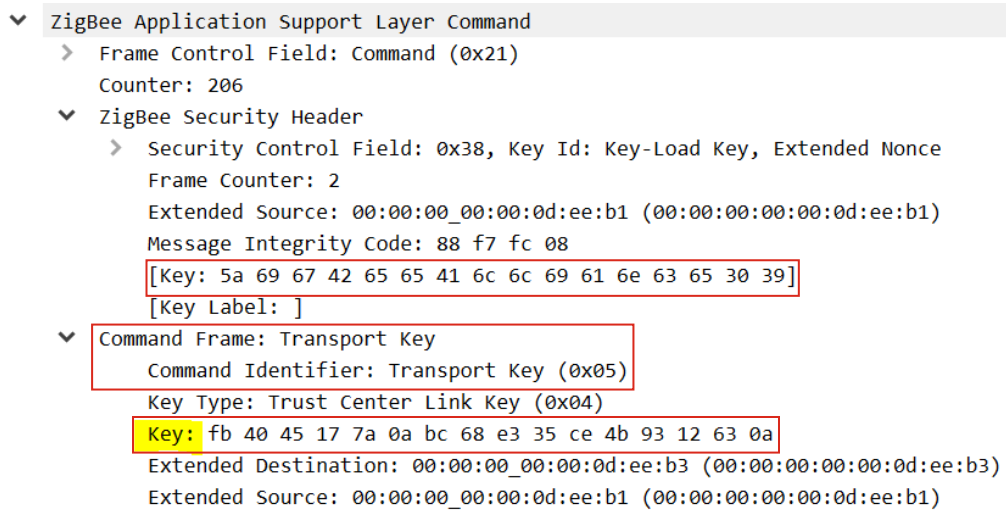
下图显示了 Request Key，其中高亮显示了用于加密 APS 层的链路 Key A（5a 69 67 42 65 65 41 6c 6c 69 61 6e 63 65 30 39）。

图 6-14. 请求密钥



下图显示了 Transport Key，其中高亮显示了用于加密 APS 层的链路 Key A（5a 69 67 42 65 65 41 6c 6c 69 61 6e 63 65 30 39）。下图显示了正在从信任中心传输到路由器的链路 Key B（fb 40 45 17 7a 0a bc 68 e3 35 ce 4b 93 12 63 0a）。

图 6-15. 传输密钥



6.3. Zigbee 路由器

Zigbee 路由器可以组建分布式网络。如果它不组建分布式网络，则可以加入由 Zigbee 协调器组建的集中式网络。

以下章节详细阐述了 Zigbee 路由器设备类型（与 Zigbee 协调器）的关联、调试、查找和绑定、属性报告以及安全密钥交换过程。

6.3.1. 调试

6.3.1.1. Zigbee 路由器/扩展灯具的网络引导

在下图中，数据包#6 显示网络引导过程从路由器设备广播 Beacon Request 开始。从协调器接收到信标帧后，路由器设备通过 MAC 关联加入网络。

MAC 关联——设备尝试通过 MAC 关联加入网络（如同首次加入未知网络）。数据包#8 至#12 显示了 MAC 关联过程。有关 MAC 关联的详细信息，请参见 MAC 关联。

图 6-16. 网络引导——路由器

No.	Source	Destination	Time	Protocol	Leng	Info
6		Broadcast	27.499082	IEEE 802.15.4	10	Beacon Request
7	0x0000		27.501054	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
8	00:00:00:00:00:0d:ee:b3	0x0000	27.639432	IEEE 802.15.4	21	Association Request, FFD
9			27.641427	IEEE 802.15.4	5	Ack
10	00:00:00:00:00:0d:ee:b3	0x0000	28.137568	IEEE 802.15.4	18	Data Request
11			28.138565	IEEE 802.15.4	5	Ack
12	00:00:00:00:00:0d:ee:b1	00:00:00:00:00:0d:…	28.141603	IEEE 802.15.4	27	Association Response, PAN: 0x2be2 Addr: 0x0401
13			28.142556	IEEE 802.15.4	5	Ack

6.3.1.2. Zigbee 路由器/扩展灯具组建分布式网络

Zigbee 路由器可以组建分布式网络。成功组建分布式网络后，广播设备通告数据包和允许入网请求，以通知其他正在搜索网络准备加入的路由器/终端设备。向终端设备/路由器发送信标请求后，父路由器以信标帧进行响应，从而进行 MAC 关联。MAC 关联成功后，终端设备/路由器即加入网络。出于安全目的，通过传输密钥在父路由器与终端设备/路由器之间传递链路密钥。有关详细信息，请参见网络安全模型。

6.3.2. 设备发现

设备通告——NWK 地址为 0x0401 的 Zigbee 路由器设备广播了数据包#16 和#17，其中显示 Device Announcement。有关详细信息，请参见 Zigbee 设备配置文件（ZDP）。

图 6-17. 设备通告

No.	Source	Destination	Time	Protocol	Leng	Info
16	0x0401	Broadcast	28.154162	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x0401, Ext Addr: 00:00:00_00:00:0d:ee:b3
17	0x0401	Broadcast	28.191112	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x0401, Ext Addr: 00:00:00_00:00:0d:ee:b3

图 6-18. 设备通告

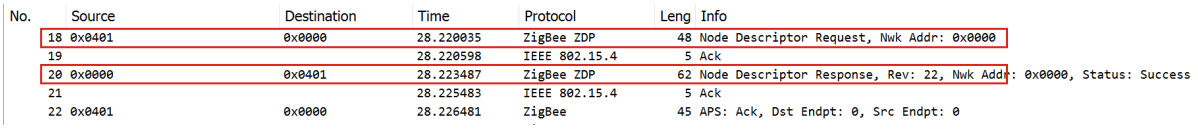
```
> Frame 16: 57 bytes on wire (456 bits), 55 bytes captured (440 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: Broadcast, Src: 0x0401
> ZigBee Network Layer Data, Dst: Broadcast, Src: 0x0401
v ZigBee Application Support Layer Data, Dst Endpt: 0, Src Endpt: 0
    > Frame Control Field: Data (0x08)
      Destination Endpoint: 0
      Device Announcement (Cluster ID: 0x0013)
      Profile: ZigBee Device Profile (0x0000)
      Source Endpoint: 0
      Counter: 140
v ZigBee Device Profile, Device Announcement, Nwk Addr: 0x0401, Ext Addr: 00:00:00_00:00:0d:ee:b3
      Sequence Number: 0
      Nwk Addr of Interest: 0x0401
      Extended Address: 00:00:00_00:00:0d:ee:b3 (00:00:00:00:00:0d:ee:b3)
    v Capability Information: 0x8e
          .... ...0 = Alternate Coordinator: False
          .... ..1. = Full-Function Device: True
          .... .1.. = AC Power: True
          .... 1... = Rx On When Idle: True
          .0.. .... = Security Capability: False
          1... .... = Allocate Short Address: True
```

6.3.3. 服务发现

节点描述符——路由器/终端设备在查找和绑定前的初始化过程中请求节点描述符，以发现网络中协调器设备的能力信息和其他信息。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

下图显示来自路由器和协调器节点的数据包#18 和#20 分别是 Node Descriptor Request 和 Node Descriptor Response。

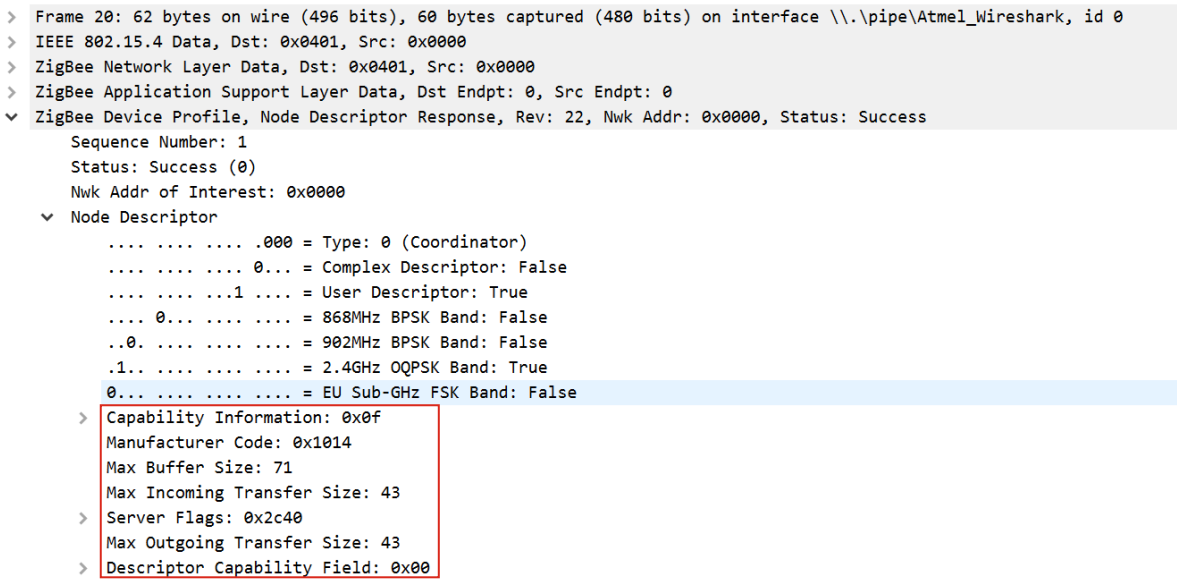
图 6-19. 节点描述符



下图显示了来自协调器设备的 Node Descriptor Response。用户可在 ZigBee Device Profile 下看到以下内容：

- 协调器节点的 Capability Information
- Max Buffer Size
- Server Flags
- Descriptor Capability Field

图 6-20. 节点描述符响应



简单描述符——从协调器接收到 Identify Query Response 后，路由器识别目标方端点并向目标方端点（协调器）发送简单描述符请求。数据包#53 和#55 分别是来自路由器和协调器设备的 Simple Descriptor Request 和 Simple Descriptor Response。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

图 6-21. 简单描述符——协调器和路由器

No.	Source	Destination	Time	Protocol	Length	Info
47	0x3c08	Broadcast	270.393782	ZigBee HA	46	ZCL Identify: Identify Query, Seq: 0
48	0x0000	0x3c08	270.399198	ZigBee HA	48	ZCL Identify: Identify Query Response, Seq: 0
49			270.401198	IEEE 802.15.4	3	Ack
50	0x3c08	0x0000	270.403622	ZigBee	43	APS: Ack, Dst Endpt: 20, Src Endpt: 35
51			270.405470	IEEE 802.15.4	3	Ack
52	0x3c08	Broadcast	270.436398	ZigBee HA	46	ZCL Identify: Identify Query, Seq: 0
53	0x3c08	0x0000	270.442286	ZigBee ZDP	47	Simple Descriptor Request, Nwk Addr: 0x0000, Endpoint: 20
54			270.444253	IEEE 802.15.4	3	Ack
55	0x0000	0x3c08	270.446654	ZigBee ZDP	102	Simple Descriptor Response, Nwk Addr: 0x0000, Status: Success
56			270.450381	IEEE 802.15.4	3	Ack
57	0x3c08	0x0000	270.453318	ZigBee	43	APS: Ack, Dst Endpt: 0, Src Endpt: 0
58			270.455157	IEEE 802.15.4	3	Ack

下图显示了来自协调器的 Simple Descriptor Response，其中列出了其支持的输入和输出簇。

图 6-22. 简单描述符响应

```
ZigBee Device Profile, Simple Descriptor Response, Nwk Addr: 0x0000, Status: Success
    Sequence Number: 3
    Status: Success (0)
    Nwk Addr of Interest: 0x0000
    Simple Descriptor Length: 54
    Simple Descriptor
        Endpoint: 20
        Profile: Home Automation (0x0104)
        Application Device: Unknown (0x0007)
        Application Version: 0x0001
        Input Cluster Count: 6
        Input Cluster List
        Output Cluster Count: 17
        Output Cluster List
```

6.3.4. 查找和绑定

用户可对目标方端点/发起方端点进行如下配置：

- Zigbee 路由器/扩展灯具——作为发起方端点
- Zigbee 协调器/组合接口——作为目标方端点

下图显示数据包#47 和#48 分别是来自路由器和协调器设备的 Identify Query Request 和 Identify Query Response。

路由器作为发起方，通过广播 Identify Query 识别目标方端点。从目标方端点接收到 Identify Query Response 后，发起方向目标设备单播 Simple Descriptor Request。然后，发起方端点搜索自身与目标方端点之间的任何匹配簇；对于找到的每个匹配项，在其绑定表中创建一个相应的条目。如果存在组绑定请求，发起方端点将配置目标方端点的组成员关系。

在收到 Identify Query Response 后，路由器识别目标方端点并请求 Simple Descriptor。数据包#53 和#55 分别是来自路由器和协调器设备的 Simple Descriptor Request 和 Simple Descriptor Response。

图 6-23. 查找和绑定——路由器

No.	Source	Destination	Time	Protocol	Length	Info
47	0x3c08	Broadcast	270.393782	ZigBee HA	46	ZCL Identify: Identify Query, Seq: 0
48	0x0000	0x3c08	270.399198	ZigBee HA	48	ZCL Identify: Identify Query Response, Seq: 0
49			270.401198	IEEE 802.15.4	3	Ack
50	0x3c08	0x0000	270.403622	ZigBee	43	APS: Ack, Dst Endpt: 20, Src Endpt: 35
51			270.405470	IEEE 802.15.4	3	Ack
52	0x3c08	Broadcast	270.436398	ZigBee HA	46	ZCL Identify: Identify Query, Seq: 0
53	0x3c08	0x0000	270.442286	ZigBee ZDP	47	Simple Descriptor Request, Nwk Addr: 0x0000, Endpoint: 20
54			270.444253	IEEE 802.15.4	3	Ack
55	0x0000	0x3c08	270.446654	ZigBee ZDP	102	Simple Descriptor Response, Nwk Addr: 0x0000, Status: Success
56			270.450381	IEEE 802.15.4	3	Ack
57	0x3c08	0x0000	270.453318	ZigBee	43	APS: Ack, Dst Endpt: 0, Src Endpt: 0
58			270.455157	IEEE 802.15.4	3	Ack

下图显示了 Simple Descriptor Response，其中详细列出了支持的输入和输出簇。

图 6-24. 简单描述符响应

```
▼ ZigBee Device Profile, Simple Descriptor Response, Nwk Addr: 0x0000, Status: Success
    Sequence Number: 3
    Status: Success (0)
    Nwk Addr of Interest: 0x0000
    Simple Descriptor Length: 54
  ▼ Simple Descriptor
      Endpoint: 20
      Profile: Home Automation (0x0104)
      Application Device: Unknown (0x0007)
      Application Version: 0x0001
      Input Cluster Count: 6
    ▶ Input Cluster List
      Output Cluster Count: 17
    ▶ Output Cluster List
```

6.3.5. 报告

下表提供了 Zigbee 协议栈中扩展彩色灯设备类型可用的客户端/服务器簇的详细信息。有关详细信息，请参见 *ZigBee Alliance Cluster Library Specification Revision 8*（075123）。有关特定设备类型的强制或可选簇的详细信息，请参见 *Matter Device Library Specification*（1.0）。

表 6-2. 支持的簇——扩展彩色灯

设备类型	簇 ID	服务器簇	客户端簇	属性标识符	属性名称
扩展彩色灯	0x0000	基本	基本	—	—
	0x0003	识别	识别	—	—
	0x0004	组	组	—	—
	0x0005	场景	—	—	—
	0x0006	开/关(1)	—	0x0000(1)	开/关(1)
	0x0008	级别控制(1)	—	0x0000(1)	当前级别(1)
	0x0300	颜色控制	—	—	—

注：

1. 在此场景中，路由器/扩展灯具设备向协调器/组合接口报告开/关（0x0006）簇的 On/Off（0x0000）属性以及级别控制（0x0008）簇的当前级别（0x0000）属性。

扩展彩色灯是一种可以打开或关闭的照明设备。用户可调节光强度，绑定的控制器设备（颜色控制器）可调整颜色。该设备支持通过色调/饱和度、增强色调、颜色循环、XY 坐标和色温来调整颜色。此外，用户还可通过绑定的占用传感器进行开/关切换。

报告属性——设备使用 Report Attributes 命令将其一个或多个属性的值报告给其他设备。各个簇定义哪些属性需要报告以及报告间隔。

图 6-25. 报告属性——路由器

No.	Source	Destination	Time	Protocol	Leng	Info
78	0x0401	0x0000	294.270097	ZigBee HA	52	ZCL: Report Attributes, Seq: 1
79			294.271856	IEEE 802.15.4	5	Ack
80	0x0000	Broadcast	296.359236	ZigBee	50	Link Status
81	0x0401	Broadcast	296.590545	ZigBee	50	Link Status
82	0x0000	Broadcast	311.478669	ZigBee	50	Link Status
83	0x0401	Broadcast	311.633395	ZigBee	50	Link Status
84	0x0000	Broadcast	326.602218	ZigBee	50	Link Status
85	0x0401	Broadcast	326.673345	ZigBee	50	Link Status
86	0x0401	0x0000	334.276770	ZigBee HA	52	ZCL: Report Attributes, Seq: 2
87			334.277767	IEEE 802.15.4	5	Ack
88	0x0401	Broadcast	341.796805	ZigBee	50	Link Status
89	0x0000	Broadcast	356.805413	ZigBee	50	Link Status
90	0x0401	Broadcast	356.876190	ZigBee	50	Link Status
91	0x0000	Broadcast	371.928857	ZigBee	50	Link Status
92	0x0401	Broadcast	371.957362	ZigBee	50	Link Status
93	0x0401	0x0000	374.278997	ZigBee HA	52	ZCL: Report Attributes, Seq: 3
94			374.282998	IEEE 802.15.4	5	Ack
95	0x0000	Broadcast	387.090623	ZigBee	50	Link Status
96	0x0401	Broadcast	387.120543	ZigBee	50	Link Status
97	0x0000	Broadcast	402.253476	ZigBee	50	Link Status
98	0x0401	Broadcast	402.282435	ZigBee	50	Link Status

下图显示了 On/Off 簇的 On/Off 属性。

图 6-26. 开/关簇——开/关属性

```
▼ ZigBee Application Support Layer Data, Dst Endpt: 20, Src Endpt: 35
  ▼ Frame Control Field: Data (0x00)
        .... ..00 = Frame Type: Data (0x0)
        .... 00.. = Delivery Mode: Unicast (0x0)
        ..0. .... = Security: False
        .0.. .... = Acknowledgement Request: False
        0... .... = Extended Header: False
    Destination Endpoint: 20
    Cluster: On/Off (0x0006)
    Profile: Home Automation (0x0104)
    Source Endpoint: 35
    Counter: 148
▼ ZigBee Cluster Library Frame, Command: Report Attributes, Seq: 2
  ▶ Frame Control Field: Profile-wide (0x18)
    Sequence Number: 2
    Command: Report Attributes (0x0a)
  ▼ Attribute Field
      Attribute: OnOff (0x0000)
      Data Type: Boolean (0x10)
      On/off Control: Off (0x00)
```

下图显示了 Cluster: Level Control 的 Current Level 属性。

图 6-27. 级别控制簇——当前级别属性

```
ZigBee Application Support Layer Data, Dst Endpt: 20, Src Endpt: 35
  Frame Control Field: Data (0x00)
      .... ..00 = Frame Type: Data (0x0)
      .... 00.. = Delivery Mode: Unicast (0x0)
      ..0. .... = Security: False
      .0.. .... = Acknowledgement Request: False
      0... .... = Extended Header: False
  Destination Endpoint: 20
  Cluster: Level Control (0x0008)
  Profile: Home Automation (0x0104)
  Source Endpoint: 35
  Counter: 147
ZigBee Cluster Library Frame, Command: Report Attributes, Seq: 1
  Frame Control Field: Profile-wide (0x18)
  Sequence Number: 1
  Command: Report Attributes (0x0a)
  Attribute Field
    Attribute: Current Level (0x0000)
    Data Type: 8-Bit Unsigned Integer (0x20)
    Current Level: 127
```

在此场景中，路由器设备和协调器设备配置如下：

- 路由器设备——报告开/关簇的开/关属性
- 协调器设备——级别控制簇的当前级别属性

6.3.6. 安全

有关集中式网络中信任中心与路由器之间的安全密钥交换，请参见安全。

6.4. Zigbee 终端设备

Zigbee 终端设备加入以下网络之一：

- 协调器——组建集中式网络
- 路由器——组建分布式网络

加入后，多传感器设备在连接到网络后开始报告传感器数据（如温度、占用状态、光照和湿度）的 ZCL 属性。

以下章节详细阐述了 Zigbee 终端设备类型（与 Zigbee 协调器）的关联、调试、查找和绑定、属性报告以及安全密钥交换过程。

6.4.1. 调试

6.4.1.1. Zigbee 终端设备/多传感器的网络引导

MAC 关联——终端设备尝试通过 MAC 关联过程加入网络（如同首次加入未知网络）。终端设备/路由器广播 `Beacon Request`，网络中的协调器/路由器发送 `Beacon Response`。MAC 关联过程在终端设备/路由器与协调器/路由器之间进行。有关详细信息，请参见 MAC 关联。

图 6-28. 网络引导——终端设备

No.	Source	Destination	Time	Protocol	Lengt	Info
6		Broadcast	36.992308	IEEE 802.15.4	10	Beacon Request
7	0x0000		36.993083	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
8	00:00:00:00:00:0d:ee:b4	0x0000	37.131442	IEEE 802.15.4	21	Association Request, RFD
9			37.132444	IEEE 802.15.4	5	Ack
10	00:00:00:00:00:0d:ee:b4	0x0000	37.631124	IEEE 802.15.4	18	Data Request
11			37.631124	IEEE 802.15.4	5	Ack
12	00:00:00:00:00:0d:ee:b1	00:00:00:00:00:0d:ee:b4	37.635136	IEEE 802.15.4	27	Association Response, PAN: 0x0733 Addr: 0x017d
13			37.635136	IEEE 802.15.4	5	Ack

6.4.2. 设备发现

设备通告——数据包#20 显示了 Zigbee 终端设备广播 NWK 地址为 0x017d 的 Device Announcement。有关详细信息，请参见 Zigbee 设备配置文件（ZDP）。

图 6-29. 设备通告——终端设备

No.	Source	Destination	Time	Protocol	Length	Info
20	0x017d	Broadcast	37.684574	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x017d, Ext Addr: 00:00:00_00:00:0d:ee:b4

图 6-30. 设备通告数据包

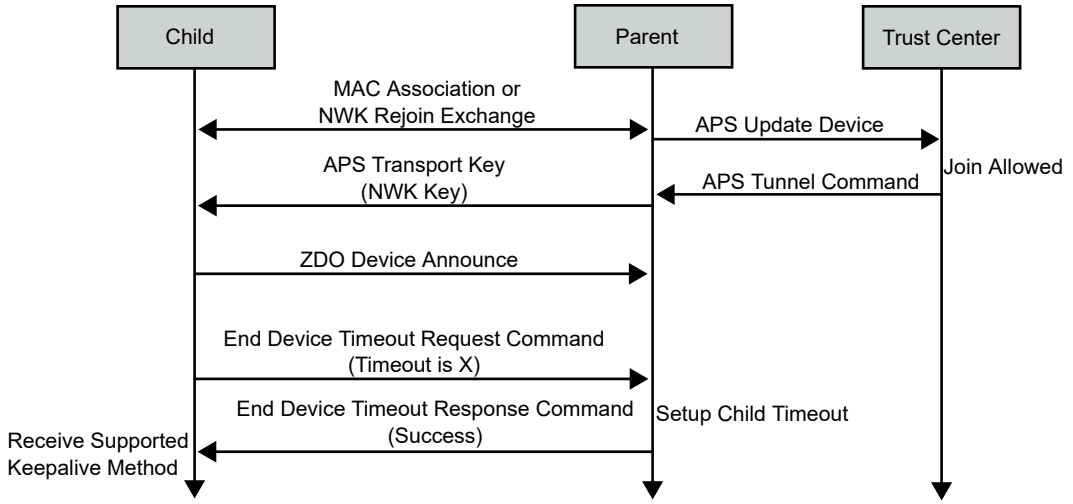
```
> Frame 20: 57 bytes on wire (456 bits), 55 bytes captured (440 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x0000, Src: 0x017d
> ZigBee Network Layer Data, Dst: Broadcast, Src: 0x017d
> ZigBee Application Support Layer Data, Dst Endpt: 0, Src Endpt: 0
v ZigBee Device Profile, Device Announcement, Nwk Addr: 0x017d, Ext Addr: 00:00:00_00:00:0d:ee:b4
    Sequence Number: 0
    Nwk Addr of Interest: 0x017d
    Extended Address: 00:00:00_00:00:0d:ee:b4 (00:00:00:00:00:0d:ee:b4)
  v Capability Information: 0x80
      .... ...0 = Alternate Coordinator: False
      .... ..0. = Full-Function Device: False
      .... .0.. = AC Power: False
      .... 0... = Rx On When Idle: False
      .0.. .... = Security Capability: False
      1... .... = Allocate Short Address: True
```

6.4.3. 终端设备超时

在加入或重新加入网络后，终端设备向其父节点发送一条含所需超时值的 End Device Timeout Request 命令。父节点在其邻近节点表中为相应的终端设备条目更新超时。父节点生成状态为 Success 且 Parent Information 字段设置为 MAC Data Poll Keepalive 方法的 End Device Timeout Response 命令。

终端设备通过发送 End Device Timeout Request 命令将其超时要求告知给其父节点。这使得父节点能够在子节点未在指定时间内与父节点通信时从邻近节点表中删除子节点条目。有关详细信息，请参见 *Zigbee Specification Revision 22 1.0*（05-3474-22）。

图 6-31. 终端设备超时序列



下图显示了 End Device Timeout 设置的完整场景。数据包#24 和#32 分别显示了来自终端设备和协调器设备的 End Device Timeout Request 和 End Device Timeout Response。

图 6-32. 终端设备超时嗅探器日志

No.	Source	Destination	Time	Protocol	Leng	Info
6		Broadcast	36.992308	IEEE 802.15.4	10	Beacon Request
7	0x0000		36.993083	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
8	00:00:00:00:00:0d:ee:b4	0x0000	37.131442	IEEE 802.15.4	21	Association Request, RFD
9			37.132444	IEEE 802.15.4	5	Ack
10	00:00:00:00:00:0d:ee:b4	0x0000	37.631124	IEEE 802.15.4	18	Data Request
11			37.631124	IEEE 802.15.4	5	Ack
12	00:00:00:00:00:0d:ee:b1	00:00:00:00:00:0d:ee:b4	37.635136	IEEE 802.15.4	27	Association Response, PAN: 0x0733 Addr: 0x017d
13			37.635136	IEEE 802.15.4	5	Ack
14	0x017d	0x0000	37.636115	IEEE 802.15.4	12	Data Request
15			37.637112	IEEE 802.15.4	5	Ack
16	0x0000	0x017d	37.640103	ZigBee	73	Transport Key
17			37.641101	IEEE 802.15.4	5	Ack
18	0x017d	0x0000	37.642098	IEEE 802.15.4	12	Data Request
19			37.643096	IEEE 802.15.4	5	Ack
20	0x017d	Broadcast	37.684574	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x017d, Ext Addr: 00:00:00_00:00:0d:ee:b4
21			37.685572	IEEE 802.15.4	5	Ack
22	0x017d	0x0000	37.689054	IEEE 802.15.4	12	Data Request
23			37.690053	IEEE 802.15.4	5	Ack
24	0x017d	0x0000	37.723371	ZigBee	56	End Device Timeout Request
25			37.725366	IEEE 802.15.4	5	Ack
26	0x017d	0x0000	37.726364	ZigBee ZDP	48	Node Descriptor Request, Nwk Addr: 0x0000
27	0x017d	Broadcast	37.730383	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x017d, Ext Addr: 00:00:00_00:00:0d:ee:b4
28	0x017d	0x0000	37.736369	ZigBee ZDP	48	Node Descriptor Request, Nwk Addr: 0x0000
29			37.737367	IEEE 802.15.4	5	Ack
30	0x017d	0x0000	38.223383	IEEE 802.15.4	12	Data Request
31			38.224385	IEEE 802.15.4	5	Ack
32	0x0000	0x017d	38.226428	ZigBee	56	End Device Timeout Response, Success
33			38.228657	IEEE 802.15.4	5	Ack

下图显示了 Parent Information 字段设置为 MAC Data Poll Keepalive 且 MAC Data Poll Keepalive 字段设置为 True 的 End Device Timeout Response。

图 6-33. 终端设备超时响应

```
> Frame 32: 56 bytes on wire (448 bits), 54 bytes captured (432 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x017d, Src: 0x0000
v ZigBee Network Layer Command, Dst: 0x017d, Src: 0x0000
  > Frame Control Field: 0x1a09, Frame Type: Command, Discover Route: Suppress, Security, Destination, Extended Source Command
    Destination: 0x017d
    <[Address: 0x017d]>
    Source: 0x0000
    <[Address: 0x0000]>
    Radius: 1
    Sequence Number: 159
    Destination: 00:00:00_00:00:0d:ee:b4 (00:00:00:00:00:0d:ee:b4)
    <[Extended Address: 00:00:00_00:00:0d:ee:b4 (00:00:00:00:00:0d:ee:b4)]>
    Extended Source: 00:00:00_00:00:0d:ee:b1 (00:00:00:00:00:0d:ee:b1)
    <[Extended Address: 00:00:00_00:00:0d:ee:b1 (00:00:00:00:00:0d:ee:b1)]>
  > ZigBee Security Header
  v Command Frame: End Device Timeout Response, Success
        Command Identifier: End Device Timeout Response (0x0c)
        Status: Success (0)
      v Parent Information: 0x01, MAC Data Poll Keepalive
            .... ...1 = MAC Data Poll Keepalive: True
            .... ..0. = End Device Timeout Request Keepalive: False
            .... .0.. = Power Negotiation Supported: False
```

6.4.4. 服务发现

路由器/终端设备在查找和绑定之前的初始化过程中请求 Node Descriptor，以发现网络中 Coordinator 设备的 Capability Information 和其他详细信息。有关详细信息，请参见 Zigbee 设备配置文件（ZDP）。

数据包#28 和#36 分别显示了来自路由器和协调器设备的 Node Descriptor Request 和 Node Descriptor Response。数据包#40 显示了终端设备对来自 Coordinator 的 Node Descriptor Response 的 APS: ACK。

图 6-34. 节点描述符——终端设备

No.	Source	Destination	Time	Protocol	Length	Info
28	0x017d	0x0000	37.736369	ZigBee ZDP	48	Node Descriptor Request, Nwk Addr: 0x0000
29			37.737367	IEEE 802.15.4	5	Ack
30	0x017d	0x0000	38.223383	IEEE 802.15.4	12	Data Request
31			38.224385	IEEE 802.15.4	5	Ack
32	0x0000	0x017d	38.226428	ZigBee	56	End Device Timeout Response, Success
33			38.228657	IEEE 802.15.4	5	Ack
34	0x017d	0x0000	38.228657	IEEE 802.15.4	12	Data Request
35			38.229655	IEEE 802.15.4	5	Ack
36	0x0000	0x017d	38.233083	ZigBee ZDP	62	Node Descriptor Response, Rev: 22, Nwk Addr: 0x0000, Status: Success
37			38.234151	IEEE 802.15.4	5	Ack
38	0x017d	0x0000	38.234151	IEEE 802.15.4	12	Data Request
39			38.234151	IEEE 802.15.4	5	Ack
40	0x017d	0x0000	38.274348	ZigBee	45	APS: Ack, Dst Endpt: 0, Src Endpt: 0
41			38.276347	IEEE 802.15.4	5	Ack

下图显示了来自 Coordinator 设备的 Node Descriptor Response。在 ZigBee Device Profile 字段下，用户可看到以下内容：

- 协调器节点的 Capability Information
- Max Buffer Size
- Server Flags
- Descriptor Capability Field

图 6-35. 节点描述符响应——终端设备

```
ZigBee Device Profile, Node Descriptor Response, Rev: 22, Nwk Addr: 0x0000, Status: Success
    Sequence Number: 1
    Status: Success (0)
    Nwk Addr of Interest: 0x0000
  Node Descriptor
        .... .... .... .000 = Type: 0 (Coordinator)
        .... .... .... 0... = Complex Descriptor: False
        .... .... ...1 .... = User Descriptor: True
        .... 0... .... .... = 868MHz BPSK Band: False
        ..0. .... .... .... = 902MHz BPSK Band: False
        .1.. .... .... .... = 2.4GHz OQPSK Band: True
        0... .... .... .... = EU Sub-GHz FSK Band: False
    Capability Information: 0x0f
        .... ...1 = Alternate Coordinator: True
        .... ..1. = Full-Function Device: True
        .... .1.. = AC Power: True
        .... 1... = Rx On When Idle: True
        .0.. .... = Security Capability: False
        0... .... = Allocate Short Address: False
    Manufacturer Code: 0x1014
    Max Buffer Size: 71
    Max Incoming Transfer Size: 43
  > Server Flags: 0x2c40
    Max Outgoing Transfer Size: 43
  > Descriptor Capability Field: 0x00
```

6.4.5. 查找和绑定

用户可对目标方端点/发起方端点进行如下配置：

- Zigbee 终端设备/多传感器——作为发起方端点
- Zigbee 协调器/组合接口——作为目标方端点

下图显示数据包#416 和#419 分别是来自终端设备和协调器设备的 Identify Query Request 和 Identify Query Response。

终端设备作为发起方，通过广播 Identify Query 识别目标方端点。从目标方端点接收到 Identify Query Response 后，发起方向目标设备单播 Simple Descriptor Request。然后，发起方端点搜索自身与目标方端点之间的任何匹配簇；对于找到的每个匹配项，在其绑定表中创建一个相应的条目。如果存在组绑定请求，发起方端点将配置目标方端点的组成员关系。

在收到 Identify Query Response（即，识别目标方端点）后，目标方端点请求 Simple Descriptor。

数据包#425 和#430 分别是来自终端设备和协调器设备的 Simple Descriptor Request 和 Simple Descriptor Response。

图 6-36. 查找和绑定——终端设备

No.	Source	Destination	Time	Protocol	Length	Info
416	0x017d	Broadcast	132.870587	ZigBee HA	48	ZCL Identify: Identify Query, Seq: 0
417	0x017d	0x0000	133.285917	IEEE 802.15.4	12	Data Request
418			133.286616	IEEE 802.15.4	5	Ack
419	0x0000	0x017d	133.288613	ZigBee HA	50	ZCL Identify: Identify Query Response, Seq: 0
420			133.290607	IEEE 802.15.4	5	Ack
421	0x017d	0x0000	133.293599	ZigBee	45	APS: Ack, Dst Endpt: 20, Src Endpt: 24
422			133.294598	IEEE 802.15.4	5	Ack
423	0x017d	0x0000	133.294598	IEEE 802.15.4	12	Data Request
424			133.295596	IEEE 802.15.4	5	Ack
425	0x017d	0x0000	133.335107	ZigBee ZDP	49	Simple Descriptor Request, Nwk Addr: 0x0000, Endpoint: 20
426			133.336105	IEEE 802.15.4	5	Ack
427	0x017d	Broadcast	133.509540	ZigBee HA	48	ZCL Identify: Identify Query, Seq: 0
428	0x017d	0x0000	133.834958	IEEE 802.15.4	12	Data Request
429			133.836744	IEEE 802.15.4	5	Ack
430	0x0000	0x017d	133.841488	ZigBee	104	Data, Dst: 0x017d, Src: 0x0000
431			133.842490	IEEE 802.15.4	5	Ack
432	0x017d	0x0000	133.843492	IEEE 802.15.4	12	Data Request
433			133.844486	IEEE 802.15.4	5	Ack
434	0x017d	0x0000	133.885790	ZigBee	45	APS: Ack, Dst Endpt: 0, Src Endpt: 0
435			133.886789	IEEE 802.15.4	5	Ack

6.4.6. 报告

下表提供了 Microchip Zigbee 协议栈中多传感器设备类型可用的客户端/服务器簇的详细信息。有关详细信息，请参见 *ZigBee Alliance Cluster Library Specification Revision 8*（075123）。有关特定设备类型的强制或可选簇的详细信息，请参见 *Matter Device Library Specification*（1.0）。

表 6-3. 支持的簇——多传感器/传感器设备类型

设备类型	簇 ID	服务器簇	客户端簇	属性标识符	属性名称
多传感器	0x0000	基本	基本	—	—
	0x0003	识别	识别	—	—
	0x0004	组	组	—	—
	0x0406	占用检测(1)	—	0x0000(1)	占用(1)
	0x0400	照度测量(1)	—	0x0000(1)	测量值(1)
	0x0402	温度测量	—	—	—
	0x0405	含水量测量	—	—	—
	0x0B05	诊断	—	—	—

注：

1. 在此场景中，终端设备/多传感器向路由器/扩展照明设备报告占用检测（0x0406）簇的占用（0x0000）属性和照度测量（0x0400）簇的测量值（0x0000）属性。

- 配置报告——使用 `Configure Reporting` 命令为簇的一个或多个属性配置报告机制。
  下图显示了数据包#436，其中指示终端设备向协调器发出的 `Configure Reporting Request`。

图 6-37. 配置报告——终端设备

No.	Source	Destination	Time	Protocol	Leng	Info
436	0x017d	0x0000	133.891775	ZigBee HA	53	ZCL: Configure Reporting, Seq: 2
437			133.892784	IEEE 802.15.4	5	Ack
438	0x017d	0x0000	134.385302	IEEE 802.15.4	12	Data Request
439			134.385302	IEEE 802.15.4	5	Ack
440	0x0000	0x017d	134.388299	ZigBee HA	52	ZCL: Configure Reporting Response, Seq: 2
441			134.390292	IEEE 802.15.4	5	Ack
442	0x017d	0x0000	134.390292	IEEE 802.15.4	12	Data Request
443			134.390292	IEEE 802.15.4	5	Ack
444	0x017d	0x0000	134.425562	ZigBee	45	APS: Ack, Dst Endpt: 20, Src Endpt: 24
445			134.427559	IEEE 802.15.4	5	Ack

`Direction` 字段指定是报告属性值还是接收属性报告。

下图显示了 ZCL 中 Reporting Configuration Record 下的 Direction 字段，该字段设置为 Received，表示协调器设备必须接收属性值。这也表明发送方（终端设备）可配置其报告机制，以向接收方（协调器）发送/报告所需的属性。根据发送方当前的绑定状态，发送方会向接收方发送报告。

在上述场景（见图 6-37）中，用户必须使用 Configure Reporting 命令配置终端设备，以向协调器设备报告 Occupancy Sensing 和 Illumination Measurement 属性（光传感器的两个属性）。

占用传感器是一种测量和检测设备，可测量并报告某个区域内的占用状态。

光传感器是一种测量和检测设备，用于测量并报告光源发出的光强度。

图 6-37 显示了 Cluster: Illuminance Measurement 的 Configure Reporting，其中终端设备向协调器报告 Attribute: Measured Value。

图 6-38. 配置报告——照度测量

```
> Frame 436: 53 bytes on wire (424 bits), 51 bytes captured (408 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x0000, Src: 0x017d
> ZigBee Network Layer Data, Dst: 0x0000, Src: 0x017d
v ZigBee Application Support Layer Data, Dst Endpt: 20, Src Endpt: 24
    > Frame Control Field: Data (0x00)
      Destination Endpoint: 20
      Cluster: Illuminance Measurement (0x0400)
      Profile: Home Automation (0x0104)
      Source Endpoint: 24
      Counter: 90
v ZigBee Cluster Library Frame, Command: Configure Reporting, Seq: 2
    > Frame Control Field: Profile-wide (0x18)
      Sequence Number: 2
      Command: Configure Reporting (0x06)
    v Reporting Configuration Record
          Direction: Received (0x01)
          Attribute: Measured Value (0x0000)
      Timeout: 90
```

下图显示了 Cluster: Occupancy Sensing 的 Configure Reporting，其中终端设备向协调器报告 Attribute: Occupancy 值。

图 6-39. 配置报告——占用检测

```
> Frame 757: 53 bytes on wire (424 bits), 51 bytes captured (408 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x0000, Src: 0x017d
> ZigBee Network Layer Data, Dst: 0x0000, Src: 0x017d
v ZigBee Application Support Layer Data, Dst Endpt: 20, Src Endpt: 19
    > Frame Control Field: Data (0x00)
      Destination Endpoint: 20
      Cluster: Occupancy Sensing (0x0406)
      Profile: Home Automation (0x0104)
      Source Endpoint: 19
      Counter: 93
v ZigBee Cluster Library Frame, Command: Configure Reporting, Seq: 5
    > Frame Control Field: Profile-wide (0x18)
      Sequence Number: 5
      Command: Configure Reporting (0x06)
    v Reporting Configuration Record
          Direction: Received (0x01)
          Attribute: Occupancy (0x0000)
      Timeout: 80
```

- 报告属性——设备使用 Report Attributes 命令将其一个或多个属性的值报告给其他设备。各个簇定义报告哪些属性以及报告间隔。

图 6-40. 报告属性——终端设备

No.	Source	Destination	Time	Protocol	Leng	Info
1068	0x017d	0x0000	294.929010	ZigBee HA	52	ZCL: Report Attributes, Seq: 7
1069			294.930010	IEEE 802.15.4	5	Ack

下图分别显示了终端设备向协调器报告 Illuminance Measurement 簇的 Measured Value 属性和 Occupancy Sensing 簇的 Occupancy 属性的详细信息。

图 6-41. 报告属性——照度测量

```
> Frame 4195: 53 bytes on wire (424 bits), 51 bytes captured (408 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x0000, Src: 0x017d
> ZigBee Network Layer Data, Dst: 0x0000, Src: 0x017d
v ZigBee Application Support Layer Data, Dst Endpt: 20, Src Endpt: 24
    > Frame Control Field: Data (0x00)
      Destination Endpoint: 20
      Cluster: Illuminance Measurement (0x0400)
      Profile: Home Automation (0x0104)
      Source Endpoint: 24
      Counter: 120
v ZigBee Cluster Library Frame, Command: Report Attributes, Seq: 32
    > Frame Control Field: Profile-wide (0x18)
      Sequence Number: 32
      Command: Report Attributes (0x0a)
    v Attribute Field
          Attribute: Measured Value (0x0000)
          Data Type: 16-Bit Unsigned Integer (0x21)
          Measured Value: 255 (=0.060474 [lx])
```

图 6-42. 报告属性——占用检测

```
> Frame 4118: 52 bytes on wire (416 bits), 50 bytes captured (400 bits) on interface \\.\pipe\Atmel_Wireshark, id 0
> IEEE 802.15.4 Data, Dst: 0x0000, Src: 0x017d
> ZigBee Network Layer Data, Dst: 0x0000, Src: 0x017d
v ZigBee Application Support Layer Data, Dst Endpt: 20, Src Endpt: 19
    > Frame Control Field: Data (0x00)
      Destination Endpoint: 20
      Cluster: Occupancy Sensing (0x0406)
      Profile: Home Automation (0x0104)
      Source Endpoint: 19
      Counter: 119
v ZigBee Cluster Library Frame, Command: Report Attributes, Seq: 31
    > Frame Control Field: Profile-wide (0x18)
      Sequence Number: 31
      Command: Report Attributes (0x0a)
    v Attribute Field
          Attribute: Occupancy (0x0000)
          Data Type: 8-Bit Bitmap (0x18)
        v Occupancy: 0x00
              .... ...0 = Occupied: False
```

6.4.7. 安全

有关集中式网络中信任中心与终端设备之间的安全密钥交换的详细信息，请参见安全。

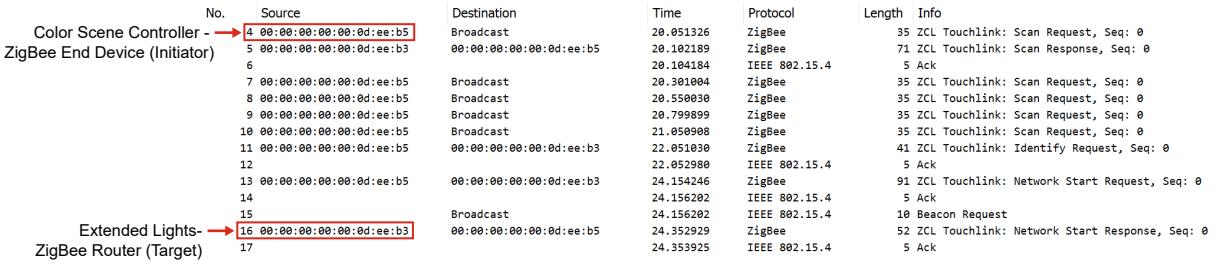
6.5. Touchlink 调试

Zigbee 协议提供了一种称为 Touchlink 的特殊调试方法，这是一种易于使用的接近度机制，用于将设备调试入网。Touchlink 调试簇提供了支持 Touchlink 调试的命令。Touchlink 调试命令集的命令标识符范围为 0x00-0x3f，并使用跨 PAN（inter-PAN）传输服务进行传输。该过程的工作原理是：

Touchlink 发起方确定目标设备（待调试）的接近度并协商/传输网络参数。Touchlink 调试过程可用于组建新网络或将节点加入现有网络。Touchlink 在称为发起方的节点上启动。ZCL 将 Touchlink 作为簇提供。发起方必须作为客户端支持 Touchlink 簇，目标节点必须作为服务器支持该簇。如果节点上需要 Touchlink 调试，可通过 Zigbee 基础设备属性 bdbCommissioningMode 使能。有关 Touchlink 调试的详细信息，请参见 *ZigBee Alliance Cluster Library Specification Revision 8*（075123）。

例如，ColorSceneController（一种终端设备类型）请求灯具通过 Touchlink 组建分布式网络，从而将灯具引入网络。若要使能 Touchlink 调试，可将颜色场景控制器靠近目标（灯具）设备，距离约为 20-30 厘米。

图 6-43. Touchlink 调试



No.	Source	Destination	Time	Protocol	Length	Info
4	00:00:00:00:00:0d:ee:b5	Broadcast	20.051326	ZigBee	35	ZCL Touchlink: Scan Request, Seq: 0
5	00:00:00:00:00:0d:ee:b3	00:00:00:00:00:0d:ee:b5	20.102189	ZigBee	71	ZCL Touchlink: Scan Response, Seq: 0
6			20.104184	IEEE 802.15.4	5	Ack
7	00:00:00:00:00:0d:ee:b5	Broadcast	20.301004	ZigBee	35	ZCL Touchlink: Scan Request, Seq: 0
8	00:00:00:00:00:0d:ee:b5	Broadcast	20.550030	ZigBee	35	ZCL Touchlink: Scan Request, Seq: 0
9	00:00:00:00:00:0d:ee:b5	Broadcast	20.799899	ZigBee	35	ZCL Touchlink: Scan Request, Seq: 0
10	00:00:00:00:00:0d:ee:b5	Broadcast	21.050908	ZigBee	35	ZCL Touchlink: Scan Request, Seq: 0
11	00:00:00:00:00:0d:ee:b5	00:00:00:00:00:0d:ee:b3	22.051030	ZigBee	41	ZCL Touchlink: Identify Request, Seq: 0
12			22.052980	IEEE 802.15.4	5	Ack
13	00:00:00:00:00:0d:ee:b5	00:00:00:00:00:0d:ee:b3	24.154246	ZigBee	91	ZCL Touchlink: Network Start Request, Seq: 0
14			24.156202	IEEE 802.15.4	5	Ack
15		Broadcast	24.156202	IEEE 802.15.4	10	Beacon Request
16	00:00:00:00:00:0d:ee:b3	00:00:00:00:00:0d:ee:b5	24.352929	ZigBee	52	ZCL Touchlink: Network Start Response, Seq: 0
17			24.353925	IEEE 802.15.4	5	Ack

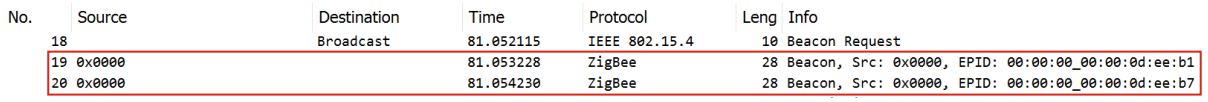
7. 应用场景示例

7.1. 个人局域网（PAN）同信道共存

同一信道上可以存在多个 Zigbee 网络。下图说明了在已有 PAN 的情况下，可以启动第二个个人局域网（PAN）。

下图显示了数据包#19 和#20，其中提供了协调器 1（扩展 PAN ID 为 0xdeeb1）和协调器 2（EPID 为 0xdeeb7）为响应路由器在同一信道中发出的 Beacon Request（数据包#18）而发送的信标帧详细信息。

图 7-1. PAN 信道共存



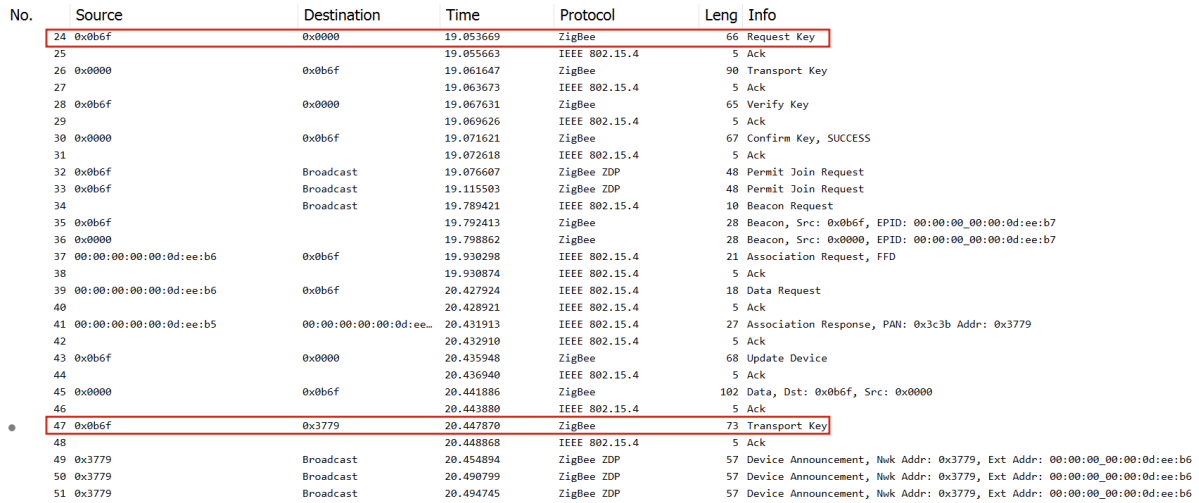
No.	Source	Destination	Time	Protocol	Leng	Info
18		Broadcast	81.052115	IEEE 802.15.4	10	Beacon Request
19	0x0000		81.053228	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b1
20	0x0000		81.054230	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b7

7.2. 端到端建立应用链路密钥

在安全网络中，当两个设备需要在安全链路上彼此通信时，必须从信任中心请求链路密钥。

下图显示了两个路由器之间的链路密钥建立过程。路由器 0x0b6f 从信任中心请求链路密钥（见数据包#24），以便与路由器 0x3779 通信。

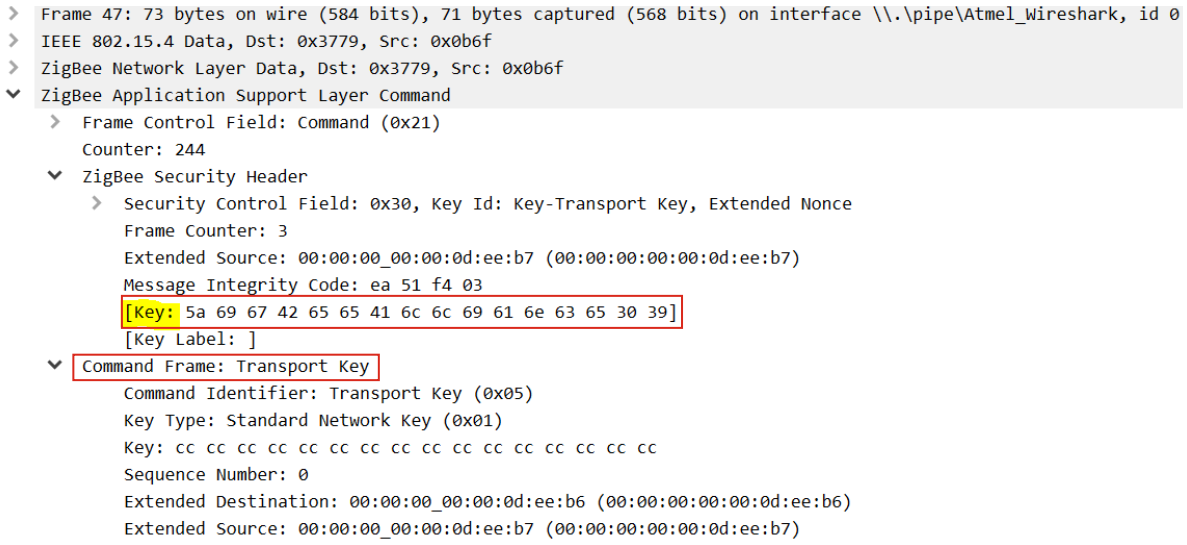
图 7-2. 两个路由器之间的链路密钥建立



No.	Source	Destination	Time	Protocol	Leng	Info
24	0x0b6f	0x0000	19.053669	ZigBee	66	Request Key
25			19.055663	IEEE 802.15.4	5	Ack
26	0x0000	0x0b6f	19.061647	ZigBee	90	Transport Key
27			19.063673	IEEE 802.15.4	5	Ack
28	0x0b6f	0x0000	19.067631	ZigBee	65	Verify Key
29			19.069626	IEEE 802.15.4	5	Ack
30	0x0000	0x0b6f	19.071621	ZigBee	67	Confirm Key, SUCCESS
31			19.072618	IEEE 802.15.4	5	Ack
32	0x0b6f	Broadcast	19.076607	ZigBee ZDP	48	Permit Join Request
33	0x0b6f	Broadcast	19.115503	ZigBee ZDP	48	Permit Join Request
34		Broadcast	19.789421	IEEE 802.15.4	10	Beacon Request
35	0x0b6f		19.792413	ZigBee	28	Beacon, Src: 0x0b6f, EPID: 00:00:00_00:00:0d:ee:b7
36	0x0000		19.798862	ZigBee	28	Beacon, Src: 0x0000, EPID: 00:00:00_00:00:0d:ee:b7
37	00:00:00:00:00:0d:ee:b6	0x0b6f	19.930298	IEEE 802.15.4	21	Association Request, FFD
38			19.930874	IEEE 802.15.4	5	Ack
39	00:00:00:00:00:0d:ee:b6	0x0b6f	20.427924	IEEE 802.15.4	18	Data Request
40			20.428921	IEEE 802.15.4	5	Ack
41	00:00:00:00:00:0d:ee:b5	00:00:00:00:00:0d:ee…	20.431913	IEEE 802.15.4	27	Association Response, PAN: 0x3c3b Addr: 0x3779
42			20.432910	IEEE 802.15.4	5	Ack
43	0x0b6f	0x0000	20.435948	ZigBee	68	Update Device
44			20.436940	IEEE 802.15.4	5	Ack
45	0x0000	0x0b6f	20.441886	ZigBee	102	Data, Dst: 0x0b6f, Src: 0x0000
46			20.443880	IEEE 802.15.4	5	Ack
47	0x0b6f	0x3779	20.447870	ZigBee	73	Transport Key
48			20.448868	IEEE 802.15.4	5	Ack
49	0x3779	Broadcast	20.454894	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x3779, Ext Addr: 00:00:00_00:00:0d:ee:b6
50	0x3779	Broadcast	20.490799	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x3779, Ext Addr: 00:00:00_00:00:0d:ee:b6
51	0x3779	Broadcast	20.494745	ZigBee ZDP	57	Device Announcement, Nwk Addr: 0x3779, Ext Addr: 00:00:00_00:00:0d:ee:b6

信任中心使用 Transport Key 命令将链路密钥发送到两个路由器。该链路密钥应用于路由器之间后续的数据交换。数据包#47 使用该链路密钥。下图显示了该链路密钥。

图 7-3. 两个路由器之间的链路密钥建立



8. Zigbee 绿色能量

以下是绿色能量（GP）基础设施设备类型：

- 绿色能量代理（GPP）设备或代理设备
- 绿色能量接收端（GPS）设备或接收设备
- 绿色能量组合（GPC）设备或组合设备

如果绿色能量设备（GPD）在附近，可以直接与接收设备进行调试。以下是两种调试方式：

- 单向调试
- 双向调试

8.1. 单向调试

- 对于单向调试，将接收设备置于调试模式，GPD 发送一条含 RxAfterTx-0 的 Commissioning 命令（见数据包#74）以及所有设备详细信息，包括设备类型、安全级别、安全密钥类型和安全密钥等（见下图）。
- 接收设备验证设备详细信息和安全密钥，并接受调试。接收设备在其接收表中为该设备创建新条目，广播 GP 配对命令（见数据包#76 和#78），并且设备以广播形式通告该新 GPD 的调试（见数据包#77 和#79）（见下图）。有关详细信息，请参见 *Zigbee PRO Green Power feature specification Basic functionality set*（Version 1.1.1）。

图 8-1. 绿色能量调试——单向调试

No.	Source	Destination	Time	Protocol	Length	Info
73	0x5ffd	Broadcast	55.120520	IEEE 802.15.4	48	Data, Dst: Broadcast, Src: 0x5ffd
74		Broadcast	64.787024	IEEE 802.15.4	40	Data, Dst: Broadcast
75	0xbeef	Broadcast	64.792848	IEEE 802.15.4	55	Data, Dst: Broadcast, Src: 0xbeef
76	0xbeef	Broadcast	64.796144	IEEE 802.15.4	76	Data, Dst: Broadcast, Src: 0xbeef
77	0x5ffd	Broadcast	64.832152	IEEE 802.15.4	55	Data, Dst: Broadcast, Src: 0x5ffd
78	0x5ffd	Broadcast	64.837176	IEEE 802.15.4	76	Data, Dst: Broadcast, Src: 0x5ffd
79	0xbeef	Broadcast	65.431176	IEEE 802.15.4	55	Data, Dst: Broadcast, Src: 0xbeef
80	0xbeef	Broadcast	69.629432	IEEE 802.15.4	48	Data, Dst: Broadcast, Src: 0xbeef
81	0x5ffd	0xbeef	69.800312	IEEE 802.15.4	48	Data, Dst: 0xbeef, Src: 0x5ffd
82			69.802312	IEEE 802.15.4	3	Ack
83	0xbeef	0x5ffd	69.804584	IEEE 802.15.4	81	Data, Dst: 0x5ffd, Src: 0xbeef
84			69.807640	IEEE 802.15.4	3	Ack
85	0x5ffd	0xbeef	69.809208	IEEE 802.15.4	43	Data, Dst: 0xbeef, Src: 0x5ffd
86			69.811048	IEEE 802.15.4	3	Ack
87	0x5ffd	Broadcast	70.281856	IEEE 802.15.4	48	Data, Dst: Broadcast, Src: 0x5ffd

8.2. 双向调试

- 对于双向调试，将接收设备置于 Commissioning 模式，GPD 发送一条含 RxAfterTx-1 的 Commissioning 命令（见数据包#145）以及所有设备详细信息，包括设备类型、安全级别、安全密钥类型和安全密钥等。
- 接收设备验证详细信息并以 Commissioning Reply 进行响应（见数据包#146 和#147）。如果在调试数据包中请求了新的安全密钥和 PAN ID，Commissioning Reply 可以包含这些内容。
- 当 GPD 接收并处理该 Commissioning Reply 后，将发送含新密钥和 PAN ID 的 Success 命令（见数据包#150）。成功解密来自 GPD 的数据包#150（Success）后，接收设备在其接收表中添加新条目，并为该设备广播 GP 配对和设备通告。有关详细信息，请参见 *Zigbee PRO Green Power feature specification Basic functionality set*（Version 1.1.1）。

图 8-2. 双向调试

No.	Source	Destination	Time	Protocol	Length	Info
133	0xbeef	Broadcast	106.345496	ZigBee	48	Link Status
134		Broadcast	108.996288	ZigBee Green Power	10	Channel Request
135	0xbeef	Broadcast	108.998000	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 2
136	0xbeef	Broadcast	109.078672	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 2
137		Broadcast	109.995840	ZigBee Green Power	10	Channel Request
138		Broadcast	110.016624	ZigBee Green Power	10	Channel Configuration
139	0xbeef	Broadcast	110.020040	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 3
140	0xbeef	Broadcast	110.060984	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 3
141	0x12345678	Broadcast	110.542648	ZigBee Green Power	41	Commissioning
142	0xbeef	Broadcast	110.546208	ZigBee GP	81	ZCL Green Power: GP Response, Seq: 4
143	0xbeef	Broadcast	110.629832	ZigBee GP	81	ZCL Green Power: GP Response, Seq: 4
144	0xbeef	Broadcast	110.654704	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 3
145	0x12345678	Broadcast	111.536240	ZigBee Green Power	41	Commissioning
146	0x12345678	Broadcast	111.557800	ZigBee Green Power	39	Commissioning Reply
147	0x12345678	Broadcast	111.559592	ZigBee Green Power	39	Commissioning Reply
148	0xbeef	Broadcast	111.563320	ZigBee GP	81	ZCL Green Power: GP Response, Seq: 5
149	0xbeef	Broadcast	111.599312	ZigBee GP	81	ZCL Green Power: GP Response, Seq: 5
150	0x12345678	Broadcast	111.657168	ZigBee Green Power	22	Success
151	0x5678	Broadcast	111.663944	ZigBee ZDP	55	Device Announcement, Nwk Addr: 0x5678, Ext Addr: ff:ff:ff:ff:ff:ff:ff:ff
152	0xbeef	Broadcast	111.667568	ZigBee GP	76	ZCL Green Power: GP Pairing, Seq: 6
153	0x5678	Broadcast	111.739280	ZigBee ZDP	55	Device Announcement, Nwk Addr: 0x5678, Ext Addr: ff:ff:ff:ff:ff:ff:ff:ff
154	0xbeef	Broadcast	111.743656	ZigBee GP	76	ZCL Green Power: GP Pairing, Seq: 6
155	0x12345678	Broadcast	111.756856	ZigBee Green Power	22	Success
156	0x5678	Broadcast	112.306512	ZigBee ZDP	55	Device Announcement, Nwk Addr: 0x5678, Ext Addr: ff:ff:ff:ff:ff:ff:ff:ff
157	0x289c	0xbeef	116.776896	ZigBee GP	48	ZCL: Read Attributes, Seq: 20
158			116.778896	IEEE 802.15.4	3	Ack
159	0xbeef	0x289c	116.781160	ZigBee GP	81	ZCL: Read Attributes Response, Seq: 20
160			116.784216	IEEE 802.15.4	3	Ack
161	0x289c	0xbeef	116.787384	ZigBee	43	APS: Ack, Dst Endpt: 242, Src Endpt: 242
162			116.789224	IEEE 802.15.4	3	Ack

8.3. 基本调试（信道配置）

- 如果设备不知道接收设备的工作信道，GPD 通过执行信道配置过程获取该信道。为获取工作信道，GPD 向接收设备发送信道请求（见数据包#134 和#137），接收设备通过信道配置命令以工作信道响应 GPD。下图显示了数据包#134、#137 和#138。
- 最初，GPD 并不知道工作信道，并在信道掩码中使能的多个信道中发送信道请求。
- GPD 在 `Channel Request` 命令的帧控制字段（Frame Control Field，FCF）中指示其是否能够接收。如果 FCF 字段的 `Auto Commissioning` 设置为 0，则使能 `RxAfterTx`，反之则禁止。
- 从同一设备发送 `Auto Commissioning = 0` 的信道请求后，GPD 接收信道配置。
- 由于发送数据包#134 信道请求数据包中的 `Auto Commissioning = 1` 且 `RxAfterTx` 被禁止，因此 GPD 不接收信道配置。而对于信道请求数据包#137，`Auto Commissioning = 0` 且 `RxAfterTx` 被使能，GPD 接收信道配置（见数据包#138）。
- GPD 在接收到该命令后将其工作信道更改为接收设备的工作信道。
- 当接收设备的工作信道与 GPD 的 RX 信道不同时，接收设备会短暂（5s）更改其信道，以便在 GPD 的 RX 信道中传送信道配置数据包。当工作信道与 RX 信道相同时，接收设备无需更改其信道。收到信道配置后，GPD 无需再发送任何信道请求，可以继续进行调试。有关详细信息，请参见 *Zigbee PRO Green Power feature specification Basic functionality set*（Version 1.1.1）。

图 8-3. 基本调试（信道配置）

No.	Source	Destination	Time	Protocol	Length	Info
133	0xbeef	Broadcast	106.345496	ZigBee	48	Link Status
134		Broadcast	108.996288	ZigBee Green Power	10	Channel Request
135	0xbeef	Broadcast	108.998000	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 2
136	0xbeef	Broadcast	109.078672	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 2
137		Broadcast	109.995840	ZigBee Green Power	10	Channel Request
138		Broadcast	110.016624	ZigBee Green Power	10	Channel Configuration
139	0xbeef	Broadcast	110.020040	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 3
140	0xbeef	Broadcast	110.060984	ZigBee GP	57	ZCL Green Power: GP Response, Seq: 3
141	0x12345678	Broadcast	110.542648	ZigBee Green Power	41	Commissioning
142	0xbeef	Broadcast	110.546208	ZigBee GP	81	ZCL Green Power: GP Response, Seq: 4

8.4. 数据发送

如果网络中存在代理设备，GPD 通过代理将数据包发送到接收设备。在这种情况下，代理设备代表 GPD 设备发送 GP 通知。下图显示了 GPD 通过代理进行的数据发送。

图 8-4. GPD 通过代理进行数据发送

No.	Source	Destination	Time	Protocol	Length	Info
1	0xbeef	Broadcast	0.000000	ZigBee	51	Link Status
2	0x55d1	Broadcast	2.423008	ZigBee GP	76	ZCL Green Power: GP Pairing, Seq: 1
3	0x55d1	Broadcast	2.499440	ZigBee GP	76	ZCL Green Power: GP Pairing, Seq: 1
4	0x55d1	Broadcast	2.502912	ZigBee GP	76	ZCL Green Power: GP Pairing, Seq: 1
5	0x55d1	Broadcast	3.142104	ZigBee GP	76	ZCL Green Power: GP Pairing, Seq: 1
6	0x70da	Broadcast	11.412616	ZigBee	51	Link Status
7	0x12345678	Broadcast	12.436600	ZigBee Green Power	22	Data, GPD Src ID: 0x12345678
8	0x5678	Broadcast	12.442520	ZigBee GP	62	ZCL Green Power: GP Notification, Seq: 1
9	0x5678	Broadcast	12.480344	ZigBee GP	62	ZCL Green Power: GP Notification, Seq: 1
10	0x5678	Broadcast	12.541600	ZigBee GP	62	ZCL Green Power: GP Notification, Seq: 2
11	0x55d1	Broadcast	12.920024	ZigBee	51	Link Status
12	0x5678	Broadcast	13.081848	ZigBee GP	62	ZCL Green Power: GP Notification, Seq: 1
13	0x5678	Broadcast	13.182536	ZigBee GP	62	ZCL Green Power: GP Notification, Seq: 2

如果网络中不存在代理设备，GPD 将数据直接发送到接收设备。下图显示了 GPD 在没有代理情况下的数据发送。

图 8-5. GPD 无代理数据发送

No.	Source	Destination	Time	Protocol	Length	Info
1	0x12345678	Broadcast	0.000000	ZigBee Green Power	14	Toggle

9. 文档版本历史

表 9-1. 文档版本历史

版本	日期	章节	说明
A	2022 年 11 月	文档	初始版本

Microchip 信息

商标

“Microchip”的名称和徽标组合、“M”徽标及其他名称、徽标和品牌均为 Microchip Technology Incorporated 或其关联公司和/或子公司在美国和/或其他国家或地区的注册商标或商标（“Microchip 商标”）。有关 Microchip 商标的信息，可访问 https://www.microchip.com/en-us/about/legal-information/microchip-trademarks。

ISBN： 979-8-3371-2567-1

法律声明

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，将来可能会发生更新。您须自行确保应用符合您的规范。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 www.microchip.com/en-us/support/design-help/client-support-services。

Microchip“按原样”提供这些信息。Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对非侵权性、适销性和特定用途的适用性的暗示担保，或针对其使用情况、质量或性能的担保。

在任何情况下，对于因这些信息或使用这些信息而产生的任何间接的、特殊的、惩罚性的、偶然的或附带的损失、损害或任何类型的开销，Microchip 概不承担任何责任，即使 Microchip 已被告知可能发生损害或损害可以预见。在法律允许的最大范围内，对于因这些信息或使用这些信息而产生的所有索赔，Microchip 在任何情况下所承担的全部责任均不超出您为获得这些信息向 Microchip 直接支付的金额（如有）。如果将 Microchip 器件用于生命维持和/或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切损害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任。除非另外声明，在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

Microchip 器件代码保护功能

请注意以下有关 Microchip 产品代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术规范。
- Microchip 确信：在正常使用且符合工作规范的情况下，Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。

产品页链接

WBZ451